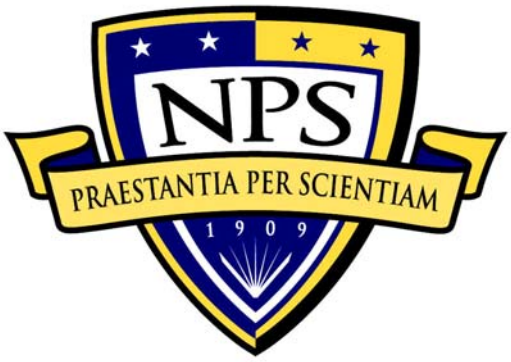

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CHEMICAL INDUSTRY SECURITY: VOLUNTARY OR MANDATORY APPROACH?

by

Paul D. Baldauf

March 2007

Co-Advisors: Thomas J. Mackin
Nadav Morag

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2007	Master's Thesis

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Chemical Industry Security: Voluntary or Mandatory Approach?	
6. AUTHOR(S) Paul D. Baldauf	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	A

13. ABSTRACT (maximum 200 words)

A successful attack on a hazardous materials storage facility has the potential to cause mass casualties and panic. Although the risk and consequences vary greatly among these sites, there are a significant number of facilities with tens of thousands of individuals who live and work in the vulnerability zone. Until P.L. 109-125 was enacted on October 4, 2006, which required the Department of Homeland Security (DHS) to issue regulations establishing risk-based performance standards, the Federal government policy for securing chemical facilities from terrorist attack relied entirely upon voluntary actions by industry.

Though it is sure to create controversy, this thesis proposes the need for new legislation that mandates standards for chemical industry security yet also addresses the economic and implementation impacts. DHS, in close partnership with the Environmental Protection Agency (EPA), is best suited to undertake this responsibility. In addition, State delegation of oversight responsibility is necessary to address the resources required to handle such a large number of sites. Public participation in preparedness and response activities is vital to reduce the fear and anxiety inherent to acts of terrorism. Inherently Safer Technology evaluations are recommended for the chemical sector through regulatory amendments to the Clean Air Act Section 112.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Chemical Facilities, Risk Management Plans, Inherently Safer Technology, Department of Homeland Security, Environmental Protection Agency, Vulnerability Assessments, New Jersey Department of Environmental Protection, Best Practice Standards, Toxic Catastrophe Prevention Act, Extraordinarily Hazardous Substance, Responsible Care Security Code	93
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CHEMICAL INDUSTRY SECURITY: VOLUNTARY OR MANDATORY APPROACH?

Paul D. Baldauf, P.E.
Assistant Director, New Jersey Department of Environmental Protection
B.S., Pennsylvania State University, 1987
M.S., Rutgers University, 1994

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2007

Author: Paul D. Baldauf

Approved by: Thomas J. Mackin
Co-Advisor

Nadav Morag
Co-Advisor

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

A successful attack on a hazardous materials storage facility has the potential to cause mass casualties and panic. There are approximately 15,000 such facilities across the country that handle these toxic and flammable substances at levels exceeding Environmental Protection Agency (EPA) regulatory thresholds. Although the risk and consequences vary greatly among these sites, there are a significant number of facilities with tens of thousands of individuals who live and work in the vulnerability zone. Until P.L. 109-125 was enacted on October 4, 2006, which required the Department of Homeland Security (DHS) to issue interim final regulations establishing risk-based performance standards, the Federal government policy for securing chemical facilities from terrorist attack relied entirely upon voluntary actions by industry.

Though it is sure to create controversy, this thesis proposes the need for new regulations that secure the chemical industry from terrorist attack. We propose new legislation that mandates standards for chemical industry security yet also addresses the economic and implementation issues associated with a typical command and control structure. DHS, in close partnership with the EPA, is best suited to undertake this responsibility. In addition, State delegation of oversight responsibility is necessary to address the resources required to handle such a large number of sites. The facilities of concern are those subject to the EPA Risk Management Program. Public participation in terms of information sharing, preparedness exercises, and protective actions is vital to reduce the fear and anxiety inherent to acts of terrorism. Inherently Safer Technology evaluations are recommended for the chemical facilities of concern through regulatory amendments to the Clean Air Act Section 112.

It is imperative that States retain the ability to be more restrictive, as warranted, to ensure that preparedness is measured in line with potential vulnerabilities. A one size fits all standard is not practical across our diverse nation. A minimum standard set by DHS will ensure a level playing field for the chemical industry with the understanding that jurisdictions with unique vulnerabilities have the ability to implement stricter standards to adequately safeguard their citizens.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. PROBLEM STATEMENT....1
B. RESEARCH QUESTION....3
C. SIGNIFICANCE OF RESEARCH....3
D. REVIEW OF LITERATURE....4
1. Existing Policy/Differing Views....4
2. Analogous Problems/Methods Applied....7
3. Strengths and Weaknesses....20
E. COMPARATIVE ANALYSIS....21
1. Introduction....21
2. European Union....22
3. Australia....25
4. Canada....26
5. Conclusions....28
F. THREAT ASSESSMENT....29
G. INHERENTLY SAFER TECHNOLOGY....31
H. STAKEHOLDER PUBLIC HEARINING....34

II. POLICY OPTIONS....37
A. INTRODUCTION....37
B. POLICY OPTION 1: NO FURTHER ACTION....40
C. POLICY OPTION 2: PRESCRIPTIVE REGULATIONS....43
D. POLICY OPTION 3: COMBINATION OF A MANDATORY AND VOLUNTARY APPROACH....44

III. METHODOLOGY....47

IV. BEST PRACTICE STANDARDS COMPLIANCE STATUS SUMMARY....51
A. INTRODUCTION....51
B. SUMMARY OF COMPLIANCE STATUS....51
C. NEXT STEPS....52
D. STANDARDS – LESSONS LEARNED....52

V. CONCLUSIONS/RECOMMENDATIONS....57
A. INTRODUCTION....57
B. LEGISLATIVE APPROACH....57
C. RESPONSIBLE AGENCY....58
D. SCOPE OF UNIVERSE....62
E. PUBLIC PREPARATION....66
F. INHERENTLY SAFER TECHNOLOGY....71

LIST OF REFERENCES....75

INITIAL DISTRIBUTION LIST....81

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost I would like to thank my wife, Jan, and children, Jill and Kate, for allowing me the opportunity to pursue this degree. I'm very appreciative of the understanding of the many weeks spent in Monterey and the hours in the living room in front of the laptop trying to make the next deadline. In addition, to my family, staff at the New Jersey Department of Environmental Protection had to pick up the slack during my time out of the office, even though I was always there through email. I would like to especially thank Director of Operations Gary Sondermeyer and Director Jill Lipoti for their encouragement throughout the last 18 months.

The knowledge and experiences of my classmates in 0503 and 0504 provided valuable insight to this thesis and I look forward to leveraging these relationships into the future as we continue our homeland security efforts. Nadav Morag and Tom Mackin provided valuable insight and all of the faculty were instrumental in motivating and driving me to complete this effort.

In summary, this thesis is the culmination of eighteen months of work which would not have been possible without the support of my family, co-workers, classmates, and faculty at the Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

In September 2003 the New Jersey Domestic Security Preparedness Task Force (Task Force) approved Security Best Practices (SBPs) for the chemical sector. The core of the SBPs is the American Chemistry Council Security Code. The SBPs are voluntary guidelines that were developed in a collaborative effort between industry, state government, and law enforcement officials. Inspections conducted by the New Jersey Department of Environmental Protection (NJDEP) revealed that seventy five percent of the sector have completed a security vulnerability assessment (SVA) and implemented the recommendations resulting from the SVA. It is important to note that the NJDEP did not review the SVAs and therefore could not make any conclusions as to their quality. The NJDEP held an Interested Party Review public hearing on December 1, 2005 to solicit comments on the existing SBPs. Representatives from industry, employee worker unions, environmental groups, and security consultants submitted comments to the NJDEP.

In order to determine compliance with the SBPs, the Task Force approved Best Practice Standards (Standards) on November 21, 2005 signed by the Attorney General, Chairman of the Task Force, and the Commissioner of the NJDEP as the Chemical Sector liaison. The Standards apply to facilities that are subject to New Jersey's Toxic Catastrophe Prevention Act or Discharge Prevention, Containment and Countermeasure program and report under certain Standard Industrial Classification (SIC) or North American Industrial Classification System (NAICS) codes related to the chemical industry. The Standards cover 157 chemical facilities and require each site to examine vulnerabilities and hazards that might be exploited by potential terrorists. The 157 facilities do not encompass all of the chemical facilities in New Jersey but rather include all of the sites storing or handling hazardous substances exceeding NJDEP regulatory threshold quantities. These assessments must be conducted by a qualified security expert and employ a methodology that has been approved by the American Institute of Chemical Engineers' Center for Chemical Process Safety. The SVAs must include, at a minimum, consideration of:

- Access and security provisions on the facility grounds (including regular testing and maintenance of security systems);
- Existing or needed security measures outside the perimeter of the facility (whether or not in the facility's control) that would reduce vulnerabilities to an attack on the facility;
- Employee and contractor background checks and other personnel measures;
- Information and cyber security; and
- Storage and processing of potentially hazardous materials.

The Standards also require the development of a prevention, preparedness, and response plan that identifies: the implementation status of all SBPs, based on its degree of security risk; and all other measures that have been implemented or are planned to be implemented to eliminate or minimize the risk of terrorist attack, to mitigate the consequences of any attack that does occur, or to respond to an attack that does occur. To the extent the plan identifies measures that have not yet been implemented, the plan shall either present the schedule for implementation of the identified measures or document that the costs of the measures are not justified by the anticipated security and public safety benefits.

The last and most controversial aspect of the Standards is a requirement to conduct a review of the practicability and the potential for adopting inherently safer technology (IST) as part of the SVA for the 45 facilities in the sector that handle extraordinarily hazardous substances (EHS). IST is defined as the principles or techniques incorporated in a covered process to minimize or eliminate the potential for an EHS accident that include, but are not limited to, the following: 1) reducing the amount of EHS material that may be released; 2) substituting less hazardous materials; 3) using EHSs in the least hazardous process conditions or form; 4) designing equipment and processes to minimize the potential for equipment failure and human error. This review must also include an analysis of whether the adoption of IST alternatives is practicable and the basis for any determination that implementation of IST is impractical.

The Standards mandate that the SVA and plans mentioned above be completed and made available to the NJDEP by March 21, 2006. Due to valid industry concerns of safeguarding the information, all assessments, plans, reports and reviews required by these Standards must be maintained on site for inspection by representatives of NJDEP or the Task Force during normal business hours. This information will provide an industry baseline and a framework in which to direct future policy in this area. Several states have established homeland security statutes and, in addition to New Jersey, both Maryland and New York have state laws or regulations specifically addressing chemical facility security.

The NJDEP planned to tier the results by compliance level to prioritize for future action. The top tier would include facilities that are determined to have ignored the Standards/SBPs or have obvious and easily exploited vulnerabilities. A middle tier would address facilities that have demonstrated a good faith effort to comply with the SBPs but have not achieved full compliance. The lowest tier would include facilities that are determined to be in full compliance with the SBPs and warrant no further action at this time.

B. RESEARCH QUESTION

The research topic will deal with the steps necessary to adequately secure the chemical industry from acts of terrorism. The research question is two fold. The first part focuses on whether the existing federal government policy, which is based upon voluntary actions by industry, is truly fulfilling its intended role of safeguarding the public from terrorist attacks on a chemical facility. If existing efforts are found to be insufficient, the second part of the question considers a mandatory approach, through rigid regulation of this sector, to balance the potential loss of life with the economic impact on industry.

C. SIGNIFICANCE OF RESEARCH

The significance of this research is demonstrated by an Environmental Protection Agency (EPA) analysis of risk management plans submitted by facilities handling

chemicals covered by the Clean Air Act Section 112. This analysis revealed that at least 123 plants reported a worst-case scenario encompassing a vulnerability zone with more than one million people.[1] Too many lives are at stake to assume that the current voluntary approach is effectively safeguarding the public. A critical evaluation of each facility's security vulnerability assessment and their response to the recommendations of that analysis is required to determine the direction of future government policy. This thesis provides federal and state governments with the information necessary to implement an effective and practical solution to this problem.

D. REVIEW OF LITERATURE

1. Existing Policy/Differing Views

The existing federal policy toward securing chemical facilities from terrorist attack relies upon voluntary actions by industry. This policy, in place prior to September 11, has not motivated the chemical industry to adequately enhance their security safeguards.[2] This opinion, however, is widely disputed by the American Chemistry Council (ACC), which adopted a Responsible Care® Security Code in June 2002. The implementation of the Security Code is mandatory for all ACC members and partner companies such as the Synthetic Organic Chemical Manufacturers Association. The ACC maintains that their members are in full compliance with the Security Code. However, the ACC recognizes that not all chemical facilities belong to the ACC, and may not have taken the same aggressive steps that member companies have taken to secure their sites.[3] The Department of Homeland Security (DHS) officially recognizes the Security Code as an Alternative Security Program for the purposes of compliance with the Maritime Transportation Security Act.

The central question in the literature is whether the existing voluntary approach to chemical industry security is safeguarding America. Frank J. Cilluffo of George Washington University offered in testimony before the U.S. House of Representatives

[1] Linda-Jo Schierow, *Chemical Plant Security* (Washington, D.C.: Congressional Research Service, 2005), 9.

[2] Ibid., 14.

[3] Martin J. Durbin, *Testimony Before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the House Committee on Homeland Security*, Congress No. 109, Session No. 1, June 15, 2005.

that regulations can create a "check in the box" mentality, where industry does just enough to meet the requirements and are further disinclined from making proactive homeland security investments.[4] If regulations are determined to be appropriate, the classification of those facilities subject to the requirements is critical to their success. Securing the United States against every conceivable vulnerability that terrorists could exploit in the chemical infrastructure would be both impossible and counterproductive.[5]

An important question is which agency is most appropriate to assume the responsibility of regulating chemical industry security. The EPA administers two federal laws that reduce risks at chemical facilities. The Emergency Response and Community Right-to-Know Act (EPCRA) and the Clean Air Act (CAA). These programs both focus on the accidental releases of hazardous chemicals. It is important to note that these programs were intended to address accidental releases only and did not specifically take into account terrorist attacks. Though the EPA originally had responsibility for chemical security, that authority has since been transferred to the DHS. The determination of responsibility is further complicated by the fact that the EPA, from an environmental standpoint, is much more familiar with the chemical industry. Furthermore, DHS lacked authority to require industry action until the 109th Congress enacted chemical security legislation as Section 550 of the DHS appropriations legislation, P.L. 109-125.

One possible option is to regulate the chemical industry through the general duty clause of the CAA. The EPA general duty clause directs industry to design and maintain a safe facility in order to prevent dangerous releases. Codifying security language into the CAA could provide the EPA with explicit authority to oversee chemical facility security. However, Richard Falkenrath of the Brookings Institution, in testimony before the U.S. Senate, pointed out that the legal merits of this claim are suspect as a practical political matter, and that any new regulatory initiative with enormous economic implications requires unambiguous statutory authorization.[6]

---

[4] Frank J. Cilluffo, *Testimony Before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Committee on Homeland Security*, Congress No. 109, Session No. 1, June 15, 2005.

[5] James Jay Carafano, *Principles for Congressional Action on Chemical Security* (Washington, D.C.:Heritage Foundation, March 31, 2006), available at: http://www.heritage.org/Research/HomelandDefense/em997.cfm (Accessed November 8, 2006).

[6] Richard A. Falkenrath, *Testimony Before the United States Senate Committee on Homeland Security and Governmental Affairs*, Congress No. 109, Session No. 1, April 27, 2005.

Another option for achieving greater security is to create incentives for voluntary compliance. Suggested incentives include federal grants, tax breaks, and other assistance from the EPA and DHS. In March 2003, and updated in March 2005, the Government Accountability Office (GAO) reviewed the overall protection of chemical infrastructure and, in particular, the existing incentives available to the chemical industry for voluntary compliance. The GAO recognized that progress has been made in securing the industry but also recommended a legislative proposal to require chemical facilities to expeditiously assess their vulnerability to terrorist attacks and, where necessary, require these facilities to take corrective action.[7] As such, the GAO recommendation combines both voluntary and regulatory approaches. If a facility's vulnerability assessment demonstrates that all necessary safeguards are in place, that facility would have achieved compliance through the existing voluntary approach. GAO only recommends a mandatory approach be implemented for those facilities that have failed to adequately safeguard their sites, proven through a vulnerability assessment.

The regulatory approach is supported by those who believe that for-profit entities are incapable of self regulation. A counter argument is that money spent on security improvements are offset by reductions in theft and insurance premiums, and an increase in public confidence. Sal DePasquale, an independent consultant, in testimony before the U.S. House of Representatives, stated that without prescriptive standards there can be no self regulation. The result of guidelines and nice sounding best practices is to create a smoke and mirrors exercise that makes it appear that something serious is being accomplished, when it is not.[8] A secondary concern voiced by sectors outside of the chemical and petroleum industries is that a regulatory approach could set a precedent for government oversight that could spread to all types of industry.

A final related issue concerns the confidentiality and protection of information collected under a regulatory or pseudo regulatory approach. Chemical facilities that have performed vulnerability assessments and have, or are in, the process of correcting deficiencies are not inclined to share this information outside of their company. A

[7] Government Accountability Office, *Protection of Chemical and Water Infrastructure* (Washington, D.C.: GAO, 2005), available at: http://www.gao.gov/htect/d05327.html (Accessed October 17, 2005).

[8] Sal DePasquale, *Testimony Before the House Committee on Homeland Security Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity*, Congress No. 109, Session No. 1, June 15, 2005.

regulatory approach would most likely require the submission of the vulnerability assessments, the decisions made to address the deficiencies, and the implementation schedule of the necessary improvements to DHS, EPA, and possibly the law enforcement community. The question of the government's ability to protect and/or exclude this information from freedom of information requests must be thoroughly addressed in the development of any new law and associated regulation. Though law enforcement has a history of protecting sensitive information, other government agencies, may find it difficult to do so. The industry perspective on releasing security information centers on the potential risk to the company's reputation among stockholders, customers, and the general public. Bobby Gilham, manager of global security at ConocoPhillips, in an article appearing in *CSO Magazine*, is concerned that any vulnerability information could be viewed as a road map for terrorists.[9]

Since September 11 the voluntary approach has resulted in an improved working relationship between industry and all levels of government. The cooperative atmosphere provides for more two way information sharing and allows the public sector easier access to private sector resources to fight the war on terrorism. Close relationships and effective communication between industry and government agencies is an essential element for success in both the prevention and response arenas. Stephen P. Bandy, Manager of Corporate Safety and Security for Marathon Ashland Petroleum fears that this level of information sharing will diminish if an agency is turned into an industry regulator through enactment of federal security legislation.[10] However, Mr. Bandy appears to contradict himself as some of the agencies he mentioned industry is working well with such as the Department of Transportation, Department of Energy, and the U.S. Coast Guard already have regulatory jurisdiction in certain aspects over the chemical and petroleum industry.

2. Analogous Problems/Methods Applied

There are two similar federal and state regulations that govern the chemical industry: the Occupational Safety and Health Administration (OSHA) and New Jersey's

[9] Todd Datz, "Capital Ideas," *CSO Magazine* (December 1, 2003), available at: http://www.csoonline.com/read/120103/ideas.html (Accessed October 17, 2005).

[10] Stephen P. Bandy, *Testimony Before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity of the House Committee on Homeland Security*, Congress No. 109, Session No. 1, June 15, 2005.

Toxic Catastrophe Prevention Act (NJTCPA). These mandatory regulations provide lessons learned for this research. The NJTCPA requires chemical facilities to submit risk management plans as a means of reducing the risk of a catastrophic release of an extraordinarily hazardous substance. The NJTCPA incorporates by reference the requirements of Section 112 of the CAA but is broader in scope and more prescriptive than the federal requirements. This program has been successful to the point that the NJTCPA is considered a model throughout the country. Since inception of the program the number of facilities handling extraordinarily hazardous substances has decreased by eighty percent. Inherently Safer Technology evaluation, mentioned later in this proposal, may have a similar effect in terms of reducing the number of facilities of concern. The OSHA standards for worker safety are also considered to be a success but the oversight and enforcement piece of the law has been subject to criticism. Specifically, due to limited resources, OSHA is not generally considered a proactive program but more often a reactive program only making a presence at a facility after an accident has occurred. The NJTCPA and the OSHA laws are typical command and control government regulations. The key lesson to be drawn from this is that the success of government regulation depends upon an effective oversight and enforcement program. As mentioned previously, companies may be unlikely to comply fully with security regulations without strict government oversight.

Due to limited resources, Federal and state regulatory agencies have been exploring other avenues to implement regulatory obligations. Third-party inspections coupled with insurance can encourage facilities throughout the supply chain to focus on risk management. The rationale for this is based upon the vast number of firms in the chemical sector. The number of audits by regulatory agencies can therefore be reduced through coordination with the private sector.

The 107th Congress enacted the Maritime Transportation Security Act of 2002 (MTSA)(P.L. 107-295), which assigned the Coast Guard the responsibility of securing our Nation's ports and those facilities located within our ports. Under MTSA, the Coast Guard has the authority to shut down a facility if it is out of compliance with the security program. There are 238 chemical facilities subject to the MTSA vulnerability assessment

and security plan requirements.[11] The State of New Jersey has a total of nine chemical and 34 petroleum facilities subject to the MTSA. The New Jersey Department of Environmental Protection (NJDEP) has worked closely with the New York and Philadelphia Coast Guard sectors, including joint inspections. This collaboration has resulted in sharing various Coast Guard checklists with the NJDEP, joint inspections, communication of general compliance rates, and specific security concerns that may require particular attention. The coupling of safety and security was supported by the Coast Guard, which testified that security auditing under MTSA often occurred while the Coast Guard was present at a chemical facility for safety reasons.[12]

Former Senator Jon Corzine, now the Governor of New Jersey, proposed strict federal security regulations for the chemical industry. However, his proposal failed after spirited Senate deliberations. Currently two chemical sector security initiatives are under consideration at the federal level: (1) the 109th Congress enacted chemical security legislation as Section 550 of the DHS appropriations legislation, P.L. 109-125, and (2) the Chemical Facility Anti-Terrorism Act of 2006 (H.R. 5695).

P.L. 109-125 requires the DHS, no later than six months after the enactment date of October 4, 2006, to issue interim final regulations establishing risk-based performance standards for security of chemical facilities and requiring vulnerability assessments and the development and implementation of site security plans for chemical facilities. It is unclear at this point the number of facilities that will be subject to these requirements as the Secretary of DHS has the discretion to limit the scope to only those that present high levels of security risk. However, it is known that facilities regulated by the Maritime Transportation Security Act of 2002, Public Water Systems, Treatment Works, Department of Defense or the Department of Energy facilities, or any facility subject to regulation by the Nuclear Regulatory Commission are exempt from these regulations. The law authorizes DHS to inspect facilities and close down those that are determined to be noncompliant. However only civil penalties are authorized for noncompliance, criminal penalties are not an option. The law is silent on numerous issues, including the

[11] John B. Stephenson, *Testimony Before the Senate Committee on Homeland Security and Governmental Affairs*, Congress No. 109, Session No. 1, April 27, 2005.

[12] Craig E. Bone, *Testimony Before the Senate Homeland Security and Governmental Affairs Committee*, Congress No. 109, Session No. 1, July 27, 2005.

criteria for weighting risks of various facilities, federal preemption of state and local right-to-know laws, how to facilitate congressional oversight, and the role of inherently safer technology.[13]

On December 22, 2006, DHS issued an advance notice of rulemaking to seek comment on both the proposed text for interim final regulations and on several practical and policy issues integral to the development of a chemical facility security program. Written comments on the proposal were due to DHS on or before February 7, 2007. Although many companies in the chemical industry have initiated voluntary security programs and have made significant capital investments in responsible security measures, the Secretary of Homeland Security has concluded that voluntary efforts alone will not provide sufficient security for the nation.[14]

The program proposed by DHS would be implemented in phases and contain the following basic steps:

- Chemical facilities fitting certain risk profiles would complete a "Top-screen" risk assessment methodology accessible through a secure Department website. The Department would use this methodology to determine if a chemical facility "presents a high level of security risk" and should be covered by the program.
- If the Department determines that a chemical facility qualifies as "high risk," the Department would require the facility to prepare and submit a Vulnerability Assessment and Site Security Plan, and would provide technical assistance to the facility as appropriate.
- Following a facility's submission of these materials, the Department would review the submissions for compliance with risk-based performance standards. The Department (or when appropriate, a DHS-certified third-party auditor) would follow up with a site inspection and audit.
- If the facility's Vulnerability Assessment or Site Security Plan is found deficient or if other problems arise, the facility could seek further technical

[13] Schierow, *Chemical Plant Security*, 47.

assistance from the Department, and could consult, object, or appeal depending on the stage of the process. If the Vulnerability Assessment and/or Site Security Plan are ultimately disapproved, the covered facility would be required to revise its plan and resubmit the materials to meet the Department's performance standards, or face the penalties and other remedies set forth in the statute.

- If the covered facility's submissions are approved, the security plan is fully implemented and the facility is otherwise in compliance, the Department would issue a Letter of Approval to document the determination. The Department would also then notify the facility of its continuing obligations – based on its level of risk – to maintain and periodically update its Vulnerability Assessment and Site Security Plan.[15]

DHS is currently considering a number of procedural questions that relate to P.L. 109-125 and specifically solicits comments on alternative approaches throughout this document. These questions will be mentioned in the order they appear in the proposal and where appropriate, background information to provide appropriate context will be provided.

A fundamental question posed by Section 550 is which facilities it covers. Section 550 specifies that the provision shall apply to chemical facilities that, at the discretion of the Secretary, present high levels of security risk.[16] The Department proposes to define a chemical facility as any facility that possesses or plans to possess a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criterion.[17] However, the DHS continues to solicit input on any alternative definitions of the term chemical facility.

The appropriate process to determine which facilities present sufficient risk is also in question. Existing chemical lists such as the EPA RMP substances, the schedule of

[14] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards* (Washington, D.C.: DHS, December 22, 2006), 2.

[15] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, 4.

[16] Ibid., 21.

[17] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, 22.

chemicals from the Convention on the Development, Production, Stockpiling and Use of Chemical Weapons and Their Destruction, the hazardous materials listed in the Department of Transportation's Hazardous Materials Regulations, and the TSA Select Hazardous Materials List are all given as potential sources of information. The DHS requests comments on appropriate information for evaluating chemical facility risks and also whether classification should be based on a hazard class approach rather than based on particular chemicals.[18] The DHS proposes a methodology system very similar to the RAMCAP "Top-screen" process to determine the high-risk facilities. The proposal requests comments as to whether the DHS should request that:

- RMP facilities complete the Top-screen;
- Certain facilities subject to the Chemical Weapons Convention complete the Top-screen;
- Any other type or description of facilities complete the Top-screen.[19]

To address human health and safety consequences, economic impacts, and mission impacts the RAMCAP "Top-screen" tool would ask the facility the following types of questions:

- Whether a toxic release worst-case scenario (as identified by the facility under the EPA Risk Management Program) might expose a residential population greater than or equal to 200,000 persons, and if so, whether the distance in such a scenario might exceed 25 miles;
- Whether a flammable release worst-case scenario (as identified by the facility under the EPA Risk Management Program) might expose a residential population greater than or equal to 1,000 persons;
- Whether the facility manufactures or stores explosive materials in sufficient quantities to result in an offsite residential exposed population;
- Whether the facility has any specified chemical weapon or chemical weapon precursors;

[18] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, 24.

[19] Ibid., 27.

- Whether the facility produces products of national economic importance or whose loss could negatively impact multiple economic sectors;
- Whether an attack on the facility could cause collateral physical damage to key transportation assets;
- Whether the facility has chemicals for which it provides 35 percent of the U.S. domestic production capacity;
- Whether the facility is the sole U.S. supplier;
- Whether the facility produces a chemical or product used in the manufacture of defense weapons;
- Whether the facility produces a chemical or product supplied to and for use by multiple defense weapons systems contractors;
- Whether the facility is a major chemical supplier (>35 percent market share) to the Department of Defense for reasons other than defense weapons systems;
- Whether a facility produces a chemical or product directly to another manufacturer, producer, or distributor for subsequent use in the manufacture of defense weapons systems;
- Whether a facility serves as a major or sole supplier to a public health, water treatment, or power generation facility.[20]

The DHS believes that the risk based performance standards mandated by Section 550 should incorporate risk-based tiering. The five following questions are posed to determine the best approach to develop such a system.

- How many risk-based tiers should the Department create?
- What should be the criteria for differentiating among the tiers?
- What types of risk should be most critical in the tiering?
- How should the performance standards differ among risk-based tiers?
- What additional levels of regulatory scrutiny (e.g. frequency of inspections, plan reviews, and updates) should apply to each tier?[21]

[20] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, Appendix A-4.

[21] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, 29.

In terms of vulnerability assessments, the DHS is considering accepting any methodologies that are certified by the Center for Chemical Process Safety (CCPS) as equivalent methodology and will review other methodologies through the Alternative Security Program (ASP) provisions.[22] ASP is defined as a third-party or industry organization program, a state or Federal government program or any aspect thereof that provides an equivalent level of security to that established by the DHS.

Several components related to background checks are being considered, including the following:

- The individuals for whom background checks would be conducted (whether that would include employees with access to restricted areas of the facility, all employees, unescorted visitors, all individuals with access to the facility or any combination of the above);
- The timing of this requirement particularly as it applies to employees (i.e., whether a background check should be conducted in association with the hiring process and, if so, how to address this requirement for current employees);
- The type of background check that should be conducted and therefore the type of personally identifiable information that would be required of these individuals, such as biometrics. Background checks might include a terrorism name check against the consolidated Terrorist Screening Database, a fingerprint-based check against terrorism and/or criminal history records, or a broader law enforcement or immigration status check;
- Whether the government should conduct these checks or whether the industry could use authorized third parties to conduct these checks.[23]

Regardless of the resolution of the background check issues, the cost and the company/individual/agency responsible to pay for this initiative is a significant concern.

Vulnerability assessments and site security plans are proposed to be updated on a regular cycle or as needed basis. The renewal timeframes are based upon the tier

[22] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, 32.

[23] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, 41.

designation of the facility with the highest tier required to complete the updates each year. Specific information relating to a particular facility may result in more or less frequent update and renewal cycles as appropriate.

The regulations issued under Section 550 will not apply to public water systems (as defined by section 1401 of the Safe Drinking Water Act); water treatment works facilities (as defined by section 212 of the Federal Water Pollution Control Act); any facilities owned or operated by the Departments of Defense and Energy; and any facilities subject to regulation by the Nuclear Regulatory Commission.[24] The regulations will also not apply to facilities covered under the Maritime Transportation Security Act (MTSA) of 2002 but there are concerns of how to address facilities subject to MTSA but not the part 105 security standards. An additional concern is the potential for the regulations to impede the Bureau of Alcohol, Tobacco, Firearms, and Explosives'' current authorities which include the purchase, possession, storage, and transportation of explosives.

The DHS intends to set forth a methodology for analyzing the costs of the interim rule. As a result input is requested on how to group facilities that will need to comply into "model facilities" for cost estimating purposes. The criteria under consideration to develop facility subgroups include:

- Should the "model facility" criteria incorporate risk-based tiering? Compliance costs may differ for a facility according to a risk-based tier.
- Should the "model facility" criteria consider the size of the facility? Larger facilities may face higher compliance costs than smaller facilities as larger facilities may need to construct longer fences or hire more guards. For the purpose of facilitating comment, facilities with six or more processes or chemicals being stored or used would be considered to be "larger."
- Should facilities that are enclosed (i.e., warehouse, enclosed manufacturing sites) be treated as a "model facility" for cost estimating purposes?

[24] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, 56.

- Should facilities that might be targeted by criminals for chemical theft or diversion be treated as a "model facility" for cost estimating purposes?
- The "model facility" estimates are expected to include current market prices of possible security enhancements that facilities may choose to undertake. Possible enhancements include, but are not limited to: Primary and secondary fences, barriers at the gate, perimeter vehicle barrier, perimeter lighting, inside lighting, CCTV system, guards, guard houses, fence line intrusion detection system, handheld radios, staging area for vehicle screenings and enhanced communication systems.[25]

The DHS is particularly concerned that a conflict or potential conflict between an approved Site Security Plan and state regulatory efforts could create ambiguity that would delay or compromise implementation of security measures at a facility. To avoid any such delays, there may be an immediate need to address potential preemption and clarify application of the law.[26] As a result, the proposal permits State or local governments, and/or covered facilities, to seek opinions on preemption from the DHS.

H.R. 5695 based on the September 29, 2006 amended version does address many of the issues not included in P.L. 109-125. The criteria to designate chemical facilities subject to H.R. 5695 include the following:

- The potential threat or likelihood that the chemical facility will be the target of terrorism.
- The potential extent and likelihood of death, injury or serious adverse effects to human health and safety or to the environment that could result from a chemical facility terrorist incident.
- The proximity of the chemical facility to population centers.
- The potential threat caused by a person obtaining a substance of concern in furtherance of an act of terrorism.

[25] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, 63.

[26] Ibid., 68.

- The potential harm to critical infrastructure, national security, and the national economy from a chemical facility terrorist incident.[27]

Based upon this criteria DHS would be required to develop regulations identifying facilities of concern, determine the risk to the nation's security associated with those facilities, set security performance standards, and establish requirements for vulnerability assessments and security plans.

In regards to federal preemption, H.R. 5695 does not preclude or deny the right of any State to adopt any chemical facility security regulation that is more stringent unless the requirement would frustrate the purposes of this title. In addition, a person, State, or local government may submit a request to the Secretary of DHS to determine whether a specific requirement is preempted by this title. It is unclear from the proposal, other than a mandated 180 timeframe for the Secretary to render a decision, the criteria that DHS would use to make a preemption determination. However, preemption is clearer in terms of IST regulation. The Committee does not believe that a State law would frustrate the purposes of this title if such State law requires a chemical facility to use or consider using a modification, process, substitution, or reduction of a substance of concern for the purposes of reducing the consequences of a terrorist incident.[28] Any decision to preempt existing state programs would likely lead to criticism that H.R. 5695 actually reduced, instead of enhanced, chemical facility security in that particular jurisdiction.

Congressional oversight is addressed through reports to Congress from the Secretary of DHS and the DHS Inspector General. No later than one year after the date of enactment, the Secretary must submit a report to Congress updating the national strategy for the chemical sector.[29] The national strategy requires an analysis of the resources necessary to implement and enforce mandatory security requirements. The Committee seeks to have this report updated and resubmitted but it is possible that the Sector Specific Plan for the Chemical Sector may satisfy this requirement. The DHS Inspector General is required, one year after the date of enactment, to submit a report to

[27] House of Representatives, *Committee Reports, House Homeland Security, House Report 109-707, Part 1 – To Accompany H.R. 5695* (Washington, D.C.: September 29, 2006), 52.

[28] Ibid., 44.

[29] Ibid., 47.

Congress on the effectiveness of implementation, and an assessment of the facility security plans required, along with any future recommendations.

IST is required to be evaluated as part of an assessment of methods to reduce the consequences of a terrorist attack. The facility may be required to implement alternative methods if and only if the Secretary determines that the methods would: significantly reduce the risk of death or injury from a terrorist release; the methods can be feasibly incorporated in the operation of the facility; and the methods would not impair the ability of the owner or operator to continue in business.[30] In the case of a determination to implement alternatives, an option to appeal the decision to the Panel on Methods to Reduce the Consequences of a Terrorist Attack is included. This panel is chaired by the Secretary and includes representatives of other Federal agencies, security experts, and the chemical industry. The Secretary must take into consideration not only the reduction in risk to a specific facility, but also the overall risk to the chemical manufacturing and production system including the possibility of the risk being shifted to other locations. In terms of feasibility and continuity of operations, consideration is given to potential loss of work time, productivity changes, and the cost and scale of proposed changes. The Committee does not intend to require facilities to adopt new, unproven, or non-existent technologies, processes, or procedures.[31] Exemptions to this section include facilities owned or operated by the Departments of Defense, Justice, or Energy or any facility that is owned or operated by a licensee or certificate holder of the Nuclear Regulatory Commission.

An appropriate definition of what is considered a chemical facility is critical to the success of any type of regulatory approach. There are three mechanisms that have commonly been proposed to select facilities that should be subject to regulation. These approaches include defining the sector by the hazardous substances on site, the adverse consequences that may result if attacked, and by industry classification. Defining the sector by companies that have a threshold quantity of listed hazardous substances is possibly the most straight forward since the Emergency Planning and Community Right to Know Act (EPCRA) and the Clean Air Act (CAA) both contain established lists. The

[30] House of Representatives, *Committee Reports, House Homeland Security, House Report 109-707, Part 1 – To Accompany H.R. 5695,* 46.

[31] Ibid., 46.

challenge is to determine which of these listed substances should be included when considering homeland security. The CAA and in New Jersey's case, NJTCPA, have been recognized as a logical starting point since the chemicals are included on these lists based upon their potential for off site consequences to human health or the environment in the event of an accidental release. However, these lists exclude potentially hazardous substances such as explosives and exempt other materials such as liquefied natural gas. Consideration would have to be given whether it is appropriate to include substances either omitted or exempted for the purposes of homeland security. It may not be adequate to simply adopt an existing list from another agency with the expectation that these are the only substances of concern.[32]

A Congressional Research Service analysis of the EPA risk management program database demonstrated that chemical manufacturing constitutes only a portion of that universe. The water and food/agriculture sectors had a similar number of facilities storing extraordinarily hazardous materials. Therefore, chemical security legislation that incorporates all EPA facilities will affect many sites not generally considered to be chemical facilities. A possible solution could be to set a threshold that would only include high risk facilities. An appropriate threshold would only capture high risk facilities and it would be expected that the majority of those facilities would be chemical manufacturers. There still would be representation from other sectors which would require the chemical facility security regulations to be flexible enough to account for different operating environments and business practices. A food sector facility subject to the requirements due to large amounts of ammonia on site for refrigeration purposes would have substantially different needs and procedures in place than a chemical manufacturer whose prime business line is the production of phosgene.

[32] Gerald Poje, *Testimony Before the Senate Homeland Security and Governmental Affairs Committee*, Congress No. 109, Session No. 1, July 13, 2005.

The likelihood and severity of the adverse consequences in the case of a terrorist attack is another potential criterion to define the chemical sector universe. DHS has taken a risk based prioritization approach for protecting critical infrastructure. A threshold consequence would assist in the determination of which facilities should receive additional resources or require additional attention. The type of data to be used for determining a consequence threshold is an issue as DHS uses a different methodology to determine the affected population resulting from a terrorist attack than what EPA uses for the risk of an accidental release. The EPA model is well established and some assert that these figures are a viable starting point for prioritizing chemical security risk.[33] However, other analysts assert that EPA figures overestimate the actual number of casualties and in one in example DHS modeling of a specific facility showed the number of persons potentially affected was much lower than projected from regulatory calculations.[34] It is also important to understand that the EPA worst case scenario is based upon an accidental release from the largest vessel at the site. Therefore, the EPA scenario would most likely underestimate the impacts of an intentional attack that targets multiple storage areas at a given location.

Industry classification is another option to determine the sector universe. The Department of Labor uses the North American Industrial Classification System (NAICS) to classify employment and economic data by industry. These codes are many times self-assigned by the facility as they select a code that most appropriately defines their business activity. The New Jersey Standards used industry classification as part of the basis to capture the facilities subject to additional security requirements. The lesson learned from the New Jersey example was that this approach captured facilities that had not been previously considered as part of the chemical sector and also omitted facilities from the mandatory requirements that were considered to be high risk sites.

3. Strengths and Weaknesses

There is a good deal of research or as some camps describe, opinions, of the appropriate solution to chemical industry security. The weaknesses and gaps of the

[33] Carol Andress, *Testimony Before the Senate Homeland Security and Governmental Affairs Committee,* Congress No. 109, Session No. 1, July 13, 2005.

[34] Robert B. Stephan, *Testimony Before the Senate Homeland Security and Governmental Affairs Committee,* Congress No. 109, Session No. 1, June 15, 2005.

existing approach centers on the lack of information available to demonstrate industry compliance with voluntary standards. The Standards compliance inspection summary described later in this thesis identifies an industry baseline to estimate the number of facilities that have not made adequate efforts to safeguard their assets. This research will provide an overall assessment of existing industry compliance and foster the development of recommendations to address security deficiencies found to exist in the chemical industry.

E. COMPARATIVE ANALYSIS

1. Introduction

The adequacy and effectiveness of the existing United States policy towards critical infrastructure protection (CIP) has been the subject of vigorous debates through all levels of government, the private sector responsible for the majority of these sites, public advocacy groups, and concerned citizens. The CIP framework has been the focal point of this debate with a growing concern that interdependencies have not been adequately addressed. Regardless of the framework, protection of information is vital to any chosen policy direction. As a result, these three areas have been chosen for this analysis. There are many other CIP issues of interest but these three in particular are the most critical to be addressed for overall strategy decisions.

The National Strategy for Homeland Security generally relies on a cooperative approach between government agencies and the private sector to determine and address vulnerabilities. Adequate metrics do not exist in most CIP sectors to gauge the success of this cooperative approach, leading to calls for strict government regulatory oversight to ensure compliance. Furthermore, interdependencies between sectors have only begun to be addressed. Protection of critical or sensitive information also varies among sectors and must be consistently applied to safeguard CIP assets. Overall, the serious consequences of a successful attack on critical infrastructure requires an in-depth evaluation of current practices.

This chapter focuses on these specific areas of CIP and overviews the strategic approaches taken by the European Union, Australia, and Canada. These strategies are then compared to the existing CIP approach in the United States with the goal of

developing policy recommendations to protect the American chemical industry from terrorist attacks. It is important to note that CIP is a very dynamic policy field and many countries are still struggling, just as we are, to determine the most effective approach. Myriam Dunn of the Swiss Federal Institute of Technology Center for Security Studies suggests that the differences in the state and the quality of the protection practices in the 14 countries she surveyed are in fact so substantial that we must reasonably ask ourselves whether we run the risk of comparing apples and oranges when trying to learn something new from them.[35] The main difficulty with the comparison of CIP policies is that countries and their various key players shape the issue in accordance with their politico-centric view of the problem. In most cases, agreement on the nature of the problem and what specifically needs to be protected is, in itself, a major challenge.

The existing CIP framework in the United States is generally a voluntary approach focused on cooperative partnerships between government and the private sector. However, there are prescriptive requirements in place for a few sectors such as the nuclear and water industry. There are ongoing discussions through various Congressional proposals that would mandate security requirements in additional areas such as the petroleum, rail transportation, pharmaceutical and biotechnology industries.

2. European Union

The Commission of the European Communities published a document in November 2005, entitled "Green Paper on a European Program for Critical Infrastructure Protection." The objective of the green paper was to solicit input from interested stakeholders concerning possible policy options for the European Program for Critical Infrastructure Protection (EPCIP). As would be expected from a topic as broad as critical infrastructure protection, this document covers a diverse range of policy issues. This analysis focuses on the framework, confidentiality, and interdependency issues previously mentioned and detail the applied methodologies.

The EPCIP framework is still under discussion with three basic options, voluntary, mandatory, or a mixture depending on the sector/issue in question. However, only a legal framework would provide a strong and enforceable legal basis for a coherent and uniform implementation of measures to protect European Critical Infrastructure, as

[35] Myriam Dunn, "The Socio-political Dimensions of Critical Information Infrastructure Protection (CIIP)," *Int. J. Critical Infrastructures* Vol. 1, Nos. 2/3 (2005): 260.

well as defining clearly the respective responsibilities of Member States and the Commission.[36] The concern is also raised that although voluntary measures provide flexibility there may not be sufficient clarity to adequately define roles and responsibilities. Proportionality of cost is a key consideration as it is crucial to maintain stability of the sectors and not negatively effect a sector's competitive position in the world market. Measures will only be proposed where a need has been identified following an analysis of existing security gaps and will be proportionate to the level of risk and the type of threat involved.[37]

A recent follow up proposal from the Commission directed the severity of the consequences of the disruption or destruction of a particular infrastructure to be assessed on the basis, where possible, of:

- Public effect (number of population affected);
- Economic effect (significance of economic loss and/or degradation of products or services);
- Environmental effect;
- Political effects;
- Psychological effects;
- Public health consequences.[38]

Article 5 of the proposal requires all critical infrastructure owners/operators to prepare operator security plans (OSPs). At a minimum the OSPs must include:

- identification of important assets;
- a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact shall be conducted;

[36] Commission of the European Communities, *Green Paper on a European Programme for Critical Infrastructure Protection* (Brussels: Commission of the European Communities, 2005), 6.

[37] Commission of the European Communities, *Communication from the Commission on a European Programme for Critical Infrastructure Protection* (Brussels: Commission of the European Communities, 2005), 3.

[38] Commission of the European Communities, *Proposal for a Directive of the Council on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection* (Brussels: Commission of the European Communities, 2006), 9.

- identification, selection and prioritization of counter measures and procedures with a distinction between permanent security measures and graduated security measures.[39]

Graduated security measures are those that are activated according to varying risk and threat levels.

The Netherlands undertook a unique approach to eliminate the transportation of chlorine by rail. The national rail system previously transported 50,000 to 60,000 tons of chlorine annually and was the target of protests for years due to the risk they pose, particularly for the villages and cities the trains passed through at night.[40] The government entered into an agreement with Akzo Nobel, the largest producer in the country, to dismantle one factory and concentrate activities at two strategically located sites where new factories were to be built. The new construction included a 65 million euro contribution from the government.[41] As a result, hazardous transports of chlorine, except for occasional small shipments, are no longer necessary in the Netherlands.

The European Commission views information sharing as critical but counters that the sharing of certain specific facts about the CI asset could be used to cause unacceptable consequences. Both at the European Union level and Member States level CIP information would be classified and access granted only on a need-to-know basis.[42] Any personnel handling classified information will have an appropriate level of security vetting by the Member State of which the person concerned is a national.[43] Designation of a senior representative to act as a Security Liaison Officer (SLO) between the owner/operator of the CI and the appropriate government authority enhances the ability to protect sensitive information. The SLO would be the main government contact to disseminate information and an active partner in developing security and contingency

[39] Commission of the European Communities, *Communication from the Commission on a European Programme for Critical Infrastructure Protection*, 10.

[40] VROM International, Netherlands Ministry of Housing, Spatial Planning and the Environment, *Safety in the Netherlands* (The Hague: Netherlands Ministry of Housing, Spatial Planning and the Environment, 2005), 10.

[41] Ibid.

[42] Commission of the European Communities, *Green Paper on a European Programme for Critical Infrastructure Protection*, 4.

[43] Commission of the European Communities, *Communication from the Commission on a European Programme for Critical Infrastructure Protection*, 6.

plans. This structure also provides a bottom up approach to regulating CI as significant responsibility is placed upon the private sector. This is not to suggest that the Commission views the SLO as working independently from other private sector partners in the determination of criticality throughout a region. There is an expectation that it is not necessary to provide equal levels of security to all assets but rather all SLOs work together with relevant authorities to safeguard the critical nodes of the CI network.

Interdependencies within and between businesses, industry sectors, geographical jurisdictions and member states are given full consideration under the European Commission's strategy. Designation of CI is at the European level due to the cross border nature of the infrastructure. Proposals for minimum protective measures, which may include mandatory standards based on the sector, are to be developed by the Commission working together with all the member states and private sector key stakeholders. An arbitration mechanism and the responsibility for verification of the designation are two components that have yet to be fully developed.

3. Australia

The Australian framework of CIP is based upon a consistent, cooperative partnership between the owners and operators of critical infrastructure and governments. The Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection enables owners and operators of critical infrastructure to share information on important issues such as business continuity, consequence management, information system attacks and vulnerabilities, e-crime, protection of key sites from attack or sabotage, chemical, biological and radiological threats to water and food supplies, and the identification and protection of offshore and maritime assets.[44]

In Australia the establishment of the TISN in April 2003 and the commitment from all parties to address CIP issues is credited, in a large part, to the private sector's confidence in how sensitive information is shared and protected. Initially, there were concerns about government freedom of information rules, the confidentiality of

[44] Australian Government Attorney's General Department – CI Owners and Operators, *Trusted Information Sharing Networks for Critical Infrastructure Protection*, available at: http://www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/RWP2D0BFCB21BFFDE9BCA2571710012CC9EC (Accessed October 25, 2006).

information, and the potential misuse of commercial-in-confidence information.[45] To address industry concerns, a Deed of Confidentiality was developed to protect sensitive information and ensure that information shared with TISN is not available for commercial or terrorist use. The TISN fosters a culture of trust where key stakeholders come together in the spirit of protecting Australia's CI. The idea of using shared information for commercial gain or as an aid to furthering terrorism is no longer an issue for the TISN members. One of the TISN principles cautions that only credible threats should be disseminated to critical infrastructure partners so as to avoid undue concern in the Australian domestic community, as well as potential tourists and investors overseas.

The Australian Critical Infrastructure Protection Modeling and Analysis (CIPMA) program maps the dependencies within and between CI sectors and facilities throughout Australia to better understand their relationship. From a natural disaster in a regional area, to the loss of a gas compressor station or electrical substation, CIPMA will become an invaluable aid for decision makers in critical infrastructure protection, counter-terrorism, and emergency management.[46] There are three sectors currently involved with CIPMA, including: banking and finance, communication, and energy. A fourth, undetermined sector, will be brought into the CIPMA program in the near future.

4. Canada

Canada focuses its efforts both on improving ways to provide reasonable protection, and also on ways to assure the continued provision of essential services. Protection and assurance can be achieved through better information collection, assessment and sharing, and through risk management. Both protection and assurance are ongoing objectives that Canada seeks to meet by building trusted partnerships. The framework of the CI strategy is based upon voluntary participation from industry stakeholders as well as from federal, provincial and territorial governments. However, Canada proposes to work with each sector in order to develop appropriate mechanisms for governance where required. Suitable mechanisms may already exist within certain sectors, while others will have to be developed, taking into account existing legislative

[45] George Mason University School of Law Critical Infrastructure Protection Program, "Trust, The Critical Ingredient in Australia's Critical Infrastructure Protection Strategy," *The CIP Report* Volume 4, No. 12 (June 2006): 4.

[46] George Mason University School of Law Critical Infrastructure Protection Program, "Trust, The Critical Ingredient in Australia's Critical Infrastructure Protection Strategy," *The CIP Report*, 3.

and regulatory environments. These governance mechanisms are to be designed with a primary goal of allowing government and the private sector to maximize coordination and integration of efforts.

Canada realizes that the process of identifying specific infrastructure components as critical also creates its own set of challenges. Since such information can be an attractive target to malicious actors, all information related to CI must be protected for reasons of national security and public safety, in addition to competitive and economic interests. Canada plans on using all of its available legislative and statutory instruments to appropriately protect CI information. Confidentiality is especially important in this context as Canada's goal is to share CI information across sectors. CI owners and operators should possess information about the critical infrastructures of others on which they depend, and the threats to their own infrastructures to carry out their business continuity activities.[47] Risk management practices can be significantly enhanced by the dissemination of information across traditional sector boundaries about potential threats and vulnerabilities that may impact previously considered unrelated CI. The Canadian Government's position is that interdependency analysis must be integrated into risk management decisions, mitigation and preparation strategies, and response and recovery activities. In addition, the Canadian Government will coordinate national efforts in interdependency research and development, which is essential to understanding this issue.[48]

Canada's Joint Infrastructure Interdependencies Research Program (JIIRP) is designed to help infrastructure owners and operators better understand the extent of their dependencies on other sectors for delivering their services and goods, and how the risks resulting from these interdependencies can be mitigated.[49] The goal of the JIIRP is to bring together all organizations with a stake in safeguarding CI to develop partnerships and methods of information exchange. Educational initiatives are also underway to promote understanding of CIP issues. An example is the Public Safety and Emergency

[47] Public Safety and Emergency Preparedness Canada, *Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection*, (Ottawa: Government of Canada, 2004), 7, available at: http://www.psepc.gc.ca/prg/em/nciap/position-paper-en.asp (Accessed October 14, 2006).

[48] Ibid., 10.

[49] George Mason University School of Law Critical Infrastructure Protection Program, "Critical Infrastructure Protection in Canada," *The CIP Report* Volume 4, No. 12 (June 2006): 16.

Preparedness Canadian Emergency Management College (CEMC). CEMC offers a CIP awareness course for both emergency management personnel and those responsible for the oversight of CI sectors. This effort is currently focused on Federal government managers but the long term goal is to provide similar training to local government and private sector employees. The interdependencies issue has only recently been widely recognized and experts are still grappling with the severity of the problem and ways to solve it.[50]

5. Conclusions

The CIP framework in the United States is very similar to that of the government agencies surveyed. A cooperative partnership with all levels of government and the private sector is the keystone to achieving a successful CIP program. However, the European Union and Canada include in their strategy, to varying degrees, the need, on a sector specific basis, to establish regulatory standards to implement and enforce minimum standards. The lesson learned from the countries surveyed is to retain government regulation as a viable alternative to address CIP in industry sectors, or portions thereof, where market forces have proven ineffective in safeguarding CI assets.

Protection of CI information is a good example of Myriam Dunn's caution of comparing apples and oranges in CIP strategies. The European Union strategy of classifying CI information does not appear as a feasible option in the United States as it would conflict with many existing regulations focused on providing transparency in government operations. However, a possible solution could rest with a simply stated but difficult to implement alternative: a critical analysis of CI information to evaluate whether the release of the data in question, from a security perspective, outweighs the public's right to be fully aware of the threat and vulnerabilities in their area. This analysis would have to be led by DHS with clear decision making matrices and a structure for consistent implementation through all levels of government and the private sector. A clear and reasonable justification as to why a particular piece of CI information

[50] Public Safety and Emergency Preparedness Canada, *Joint Infrastructure Interdependencies Program* (Ottawa: Government of Canada, 2004), available at: http://www.psepc.gc.ca/prg/em/jiirp/index-en.asp (Accessed October 14, 2006).

is protected from public dissemination is the first step in assuring the public that the CIP information strategy is effective and truly focused on the data that can be used for malicious purposes.

Australia's CIPMA program, although only in effect for three sectors at this point, is a significant step forward in understanding the interdependencies that exist across CI sectors. The existing close relationship between the United States and Australia is an excellent opportunity to leverage the CIPMA experiences to formulate an effective homeland strategy. Further research is required to determine if Canada's strategy to provide CI threats and vulnerabilities across sectors is appropriate for use in the United States. Though, on the surface this may appear beneficial, it may result in information overload on the private sector until each facility is fully aware and has addressed their own weaknesses. The reality is that the DHS does not have adequate interdependency methodology in place for CIP. In general, the CI focus on vulnerability and risk management has been, at worst, facility specific and, at best, sector specific. The next crucial step forward is the recognition of the vital nature of interdependencies across CI sectors and a framework to incorporate such into risk assessments. The DHS Risk Analysis and Management for Critical Asset Protection (RAMCAP) program provides the potential to standardize risk assessments across CI sectors. However, RAMCAP must also address interdependencies to provide an accurate picture of the challenges to protection, business continuity, and economic survival facing each CI facility.

F. THREAT ASSESSMENT

The DHS lacks credible, specific, or corroborated intelligence indicating a direct threat to the U.S. chemical sector by terrorist groups.[51] Recently, however, al-queda affiliated insurgent groups in Iraq have targeted chemical facilities to enhance the lethality of their attacks. As such, a plausible threat remains as a successful attack against chemical facilities has the potential to meet terrorist goals such as mass casualties, panic, and reduced confidence in the government's ability to protect the population. Economic effects are generally considered to be less substantial due to redundant capabilities and

[51] Department of Homeland Security, Office of Intelligence and Analysis/Office of Infrastructure Protection, Homeland Infrastructure Threat & Risk Analysis Center (HITRAC), *Strategic Sector Assessment (U//FOUO) Chemical Sector* (Washington, D.C.: DHS, October 30, 2006), 3. FOUO

product stockpiles, and the highly complex and distributed supply chain makes it very difficult to shut down the chemical industry by interruption at a single point. However, any vulnerability analysis must take into account an attack at a dominant node or link of the supply chain of a critical chemical with the potential of bringing production to a standstill. In order to achieve widespread interruption in production for an extended period, multiple interruptions at different locations would have to occur at dominant nodes or links.[52] Even the worst accidents on record (Bhopal, Toulouse, Texas City) did not result in a situation in which the supply of the chemical or fertilizer in question could not be made available through other sources in a short time.[53] This was evident during the aftermath of hurricanes Rita and Katrina which damaged more than 50 chemical plants and other infrastructure on which the chemical sector depends but did not cause catastrophic harm to the U.S. economy.[54] In addition, the potential to steal or divert chemical sector assets for use in chemical and explosive based attacks is also a concern.

A direct attack on a chemical facility with the intent to release toxic chemicals is not unprecedented.[55] However, the effectiveness of such an attack is limited by weather conditions, wind direction, existing mitigation capabilities, and specific knowledge of the facility in question. As previously discussed the extensive availability of open source information pertaining to chemical facilities is a vulnerability that enhances a terrorist's operational planning capability. The facility itself is not the only area that must be protected as the chemical sector relies heavily on maritime, rail, and road transportation for raw materials and the distribution of finished products.

Scenarios of concern, similar to the design basis threat in use in the nuclear sector, include improvised explosive devices (IEDs), VBIEDs, rocket-propelled grenades, improvised rockets, and mortars. The worst case consequence scenarios developed by EPA generally over estimate the actual results of a terrorist attack. This is due to the fact that they do not take into account safety features at the facility or limit the effects to the

[52] Committee on Assessing Vulnerabilities Related to the Nation's Chemical Infrastructure, National Research Council, *Terrorism and the Chemical Infrastructure: Protecting People and Vulnerabilities* (Washington, D.C.: The National Academies Press, 2006), 25, available at: http://www.nap.edu/catalog/11597.html (Accessed December 1, 2006).

[53] Ibid., 28.

[54] Department of Homeland Security, *Strategic Sector Assessment (U//FOUO) Chemical Sector*, 3.

[55] Ibid., 4.

population in the downwind direction. The release consequences will be affected by the source (e.g., release rate, release duration, and toxicity), meteorology (wind speed, wind direction, atmospheric stability, precipitation), and population (e.g., population distribution and structural protection; response action) factors.[56] However, since EPA's worst case scenarios base the release on the failure of the largest single vessel at the site, the estimate may become more accurate if multiple simultaneous vessels are breached.

G. INHERENTLY SAFER TECHNOLOGY

The requirement to evaluate Inherently Safer Technology (IST) has been historically a very controversial issue in terms of safety and security initiatives within the chemical industry. The concept of IST was introduced approximately thirty years ago as a process safety initiative. IST studies have been widely performed by industry since that time. As a result of the events of September 11, the application of IST as a method to reduce the risk of a terrorist attack has gained significant support. The most desirable solution to preventing a chemical release is to reduce or eliminate the hazard where possible, not simply to control it.[57]

Advocates of IST cite the inherent overlap between process safety and homeland security and note that the implementation of such measures would directly reduce security risks since the hazard would be potentially replaced or reduced. Industry associations have generally been resistant to legislation mandating the evaluation and/or implementation of IST. Industry takes the position that decisions regarding IST are weighed on a process and facility basis, and are routinely considered by process engineers when optimizing and assessing process change.[58] There are also concerns for the potential of negative safety impacts such as increasing transportation of hazardous materials and transferring risk to other areas that may result if IST approaches are incorrectly implemented. This leads back to the question of whether regulation of IST is more appropriate in an agency staffed with process safety experts as opposed to

[56] Committee on Assessing Vulnerabilities Related to the Nation's Chemical Infrastructure, National Research Council, *Terrorism and the Chemical Infrastructure: Protecting People and Vulnerabilities*, 30.

[57] Committee on Assessing Vulnerabilities Related to the Nation's Chemical Infrastructure, National Research Council, *Terrorism and the Chemical Infrastructure: Protecting People and Vulnerabilities*, 106.

[58] Martin J. Durbin, *Testimony Before the Senate Homeland Security and Governmental Affairs Committee*, Congress No. 109, Session No. 1, July 13, 2005.

individuals with experience in homeland security. Critics are likely to question EPA and OSHA homeland security expertise but just as likely will question the background or readiness of DHS staff to make complex chemical risk assessments.

The potential to effectively implement IST occurs during the design process when there remains a great deal of flexibility in terms of materials, operations, and physical location. However, major enhancements to the inherent safety of existing chemical plants have been reported.[59] Unfortunately, many times it is not clear which of several process alternatives is inherently safer. Because nearly all chemical processes have a number of hazards associated with them, an alternative which reduces one hazard may increase a different hazard.[60]

Information is not available to fully answer the question of how many chemicals defined by the EPA as extraordinarily hazardous substances have scientifically proven alternatives that increase safety, reduce risk, and operate at least as effectively, in terms of cost and end product, as the substance being replaced. However, some examples of New Jersey IST successes include:

- Over twenty wastewater facilities have switched from using chlorine to sodium hypochlorite for disinfection of their treated wastewater.
- Four electric generation and cogeneration plants substituted anhydrous ammonia with aqueous ammonia for use in their air pollution control systems.
- One facility switched from chlorine to bromochlorohydantoin for use as an algaecide in treating cooling water.
- One facility switched from bulk storage of liquid sulfur trioxide to on-site generation of gaseous sulfur trioxide for direct consumption into the process.
- One facility switched from bulk storage of chlorine to on-site generation of ozone for disinfection of potable water.

[59] Robert E. Bollinger, David G. Clark, Arthur M. Dowell III, Rodger M. Ewbank, Dennis C. Hendershot, William K. Lutz, Steven I. Meszaros, Donald E. Park and Everett D. Wixom, *Inherently Safer Chemical Processes, A Life Cycle Approach* (New York, New York: American Institute of Chemical Engineers, 1996), 16.

[60] Ibid., 17.

- Another facility is proposing to switch from bulk storage of chlorine to on-site generation of chlorine dioxide for paper bleaching.

For a particular process or chemical product being manufactured, substitution may not be a feasible alternative, but use of one or more of the other three IST techniques could provide a feasible reduction in risk. The National Research Council has recommended to DHS as part of science and technology investment, to research the development of inherently safer alternatives and apply them to current processes that require high volumes of toxic or flammable materials.[61]

It would be difficult to provide a defined list of required specific ISTs or equipment because each chemical process must be evaluated individually. Also, many processes are proprietary. It is possible to provide guidance on technologies or equipment for consideration by facilities in their process. This guidance could be prepared with input and assistance from academia, government, industry, and organizations such as the Center for Chemical Process Safety, the American Chemistry Council, and the American Petroleum Institute. Rather than accepting the hazards in a process, and then adding on safety systems and layers of protection to control those hazards, the process designer is challenged to reconsider the process and eliminate the hazards.[62] Publicizing the virtues of IST beyond the process safety community and into the broader chemistry and chemical engineering community is necessary.[63]

Performing an IST evaluation and implementing IST or other risk reduction measures provide several positive benefits resulting in a more stable business plan for a facility. First of all, the reduction in risk lowers potential liabilities. This has the secondary benefit of increasing the surrounding community's perception, confidence, and acceptance of the facility. Many IST alternatives, which have an initial capital cost, result in lower operating costs in areas such as maintenance, operations, and emergency response requirements. However, even when the benefits of an inherently less safe technology justify its use, we should always continue to look for inherently safer

[61] Committee on Assessing Vulnerabilities Related to the Nation's Chemical Infrastructure, National Research Council, *Terrorism and the Chemical Infrastructure: Protecting People and Vulnerabilities,* 51.

[62] Bollinger, Clark, Dowell, Ewbank, Hendershot, Lutz, Meszaros, Park, and Wixom, *Inherently Safer Chemical Processes, A Life Cycle Approach*, 24.

[63] Ibid., 128.

alternatives. Technology continues to evolve and advance, and inherently safer alternatives which are not economically attractive today may be very attractive in the near future.[64] If the risk of release can be eliminated or substantially reduced, the facility would become less attractive to a terrorist and thus less likely a terrorist target. Reducing or eliminating the risk of a release, whether caused by terrorism or occurring accidentally, would avoid business losses from a production shutdown following the incident. All of these serve to provide the facility a more stable business plan.

H. STAKEHOLDER PUBLIC HEARINING

On December 1, 2005 the New Jersey Department of Environmental Protection held a public hearing to solicit comments on chemical plant safety. Specifically, the NJDEP was interested in suggestions on areas where the Chemical Sector Best Practices could be strengthened and under what circumstances inherently safer technology should be required. This was the first public hearing of this type for any security best practices endorsed by the New Jersey Domestic Security Preparedness Task Force and approved by the Governor. Written comments were accepted until January 5, 2006. A wide variety of stakeholders were represented at the hearing, including the following list of organizations that offered testimony.

- Chemistry Council of New Jersey
- New Jersey Assemblyman – District 3
- American Chemistry Council
- New Jersey Work Environment Council
- Akzo Nobel
- Lubrizol Dock Resins
- New Jersey Public Interest Research Group
- United States Steel Workers
- Noveon Specialty Chemicals
- Air Products and Chemicals
- National Paint and Coatings Association

[64] Bollinger, Clark, Dowell, Ewbank, Hendershot, Lutz, Meszaros, Park, and Wixom, *Inherently Safer Chemical Processes, A Life Cycle Approach*, 19.

- New Jersey Sierra Club
- New Jersey Environmental Foundation
- BASF Corporation
- New Jersey State Industrial Union Council
- Public Employees for Environmental Responsibility
- Cease Fire New Jersey

In general, all parties in attendance were appreciative of the opportunity to comment on the Chemical Sector Best Practices. The Chemistry Council of New Jersey estimated that, since September 11, over a hundred million dollars had been spent by their members in New Jersey to harden facilities, increase security and put assets into place to protect workers and the public.[65] These results demonstrated that a cooperative relationship was much better than a prescribed regulatory regimen because the issue was too important to leave to regulations.[66] A misdirected regulatory approach which penalizes those facilities that have voluntarily safeguarded their assets has the potential to drive those manufacturing jobs out of New Jersey. Criticism of the Best Practices centered around the fact that there was no participation mechanism to allow workers, union representatives, environmental groups, and members of the public to play a role in the development and implementation of this initiative. Paul Renner, representing the United States Steel Workers, emphasized the vital necessity of training for workers to equip them with skills and language necessary to play fully in the process and be able to articulate their concerns and recommendations for making their facilities less vulnerable to consequences of an intentional act.[67] The workers who run the processes often know as much, if not more, about the intimacies of the process than the engineers themselves. Suzanne Leta, an advocate with the New Jersey Public Interest Research Group expressed concerns that the Responsible Care program is a product of industry self

[65] Hal Bozarth, *Testimony Before the New Jersey Department of Environmental Protection in the matter of Chemical Security Best Practices*, Trenton, NJ, December 1, 2005.

[66] Ibid.

[67] Paul Renner, *Testimony Before the New Jersey Department of Environmental Protection in the matter of Chemical Security Best Practices*, Trenton, NJ, December 1, 2005.

regulation and, as a voluntary industry endeavor, the chemical industry is not accountable to the public or to the government to provide complete safety.[68]

In terms of inherently safer technologies (IST), the American Chemistry Council took the position that it was not appropriate to address this concern through a regulatory process. They cited a variety of reasons including the lack of established measurement methodologies and the complexity of chemical processes. Inherent safety is not fully understood, so regulating it and forcing change against accepted good engineering practices with a long history of safe performance is not recommended.[69] One facility manager raised the concern that IST is already part of their evaluation process and to require the resources to be committed to existing product formulations without consideration for the benefit, merely weakens the overall security effort. Customers are not willing to pay extra for inherently safer ingredients.[70] The separation of IST and security requirements was also mentioned as it was posited that New Jersey should continue to address implementing best security measures but leave issues concerning chemical processes separate from the issue of plant security. IST is a process safety issue and does not belong in security requirements.[71]

[68] Suzanne Leta, *Testimony Before the New Jersey Department of Environmental Protection in the matter of Chemical Security Best Practices*, Trenton, NJ, December 1, 2005.

[69] Jamie Conrad, *Testimony Before the New Jersey Department of Environmental Protection in the matter of Chemical Security Best Practices*, Trenton, NJ, December 1, 2005.

[70] Larry Swetland, *Testimony Before the New Jersey Department of Environmental Protection in the matter of Chemical Security Best Practices*, Trenton, NJ December 1, 2005.

[71] Clyde Miller, *Testimony Before the New Jersey Department of Environmental Protection in the matter of Chemical Security Best Practices*, Trenton, NJ December 1, 2005.

II. POLICY OPTIONS

A. INTRODUCTION

There are three proposed alternative solutions. A critical evaluation of the voluntary efforts by industry to date may demonstrate that the public is adequately protected and no further action is required – this constitutes the first alternative. The sources used in this evaluation included the Department of Homeland Security, Congressional Research Service, National Research Council, Government Accountability Office, testimony of industry experts, success/failure of analogous regulatory programs, and personal experience regulating the New Jersey chemical industry. If security deficiencies are found to exist in the industry a second alternative is to assemble a plan for a more effective policy through regulation. Regulation in this case would be typical command and control prescriptive language. General examples of the requirements could include specific height requirements for perimeter fencing, detailed procedures for background checks of all individuals entering the site, and cyber protocols complying with a nationally accepted standard. In simplistic terms a voluntary approach requires considering security upgrades whereas regulations mandate implementation of upgrades. Regulation would also add another element to the process, government inspection and enforcement of the law. A third and final alternative is a combination of the voluntary and mandatory approach to achieve an acceptable standard of security throughout the chemical sector. To provide consistency and fairness to industry regulation should be at the federal level, but could be achieved at the State level if necessary. This alternative would require little or no immediate action from companies that have voluntarily safeguarded their facility but would include prescriptive standards for those that were found to be non compliant. There is an assumption that is stated in the National Strategy for Homeland Security that rigid regulation has proven to be an inefficient means of meeting objectives.[72] However, Dr. Linda Greer of the Center for American Progress

[72] Office of Homeland Security, *National Strategy for Homeland Security* (Washington, D.C.: Government Printing Office, 2002), 64.

posits that the issue is not voluntary versus mandatory approaches but the question is whether the critical infrastructure is adequately protected.[73]

The potential strengths and weaknesses of each policy option will be measured by the following five criteria: potential to adequately safeguard the industry, requirements are practical and economically feasible taking into account the potential risk posed and the financial ability to mitigate such, addresses the varied concerns of all stakeholders to the maximum extent possible, the ability to efficiently inspect and evaluate compliance at each site, and a communicable metric to determine effectiveness.

A key issue that must be determined with these alternatives is which governmental agency should be given the responsibility to oversee this sector and at what level. The criterion to be considered in this case is the feasibility of an agency undertaking this responsibility. This capacity will be based on technical expertise, experience, resources, and other related factors necessary to provide adequate oversight of the chemical industry. Options include the DHS, the EPA, or possibly a delegation of such authority to state government similar to some existing environmental protection laws. Analysts have suggested an approach combining the skills of both DHS and EPA in overseeing chemical facility security.[74] Since the population potentially affected by a chemical release generally resides near specific facilities, some experts may argue that chemical facility concerns should be dealt with by state or local authorities. Delegation to the state level would reduce the burden placed on federal agencies. Other experts claim the potentially catastrophic nature of a terrorist attack and the widespread distribution of chemical facilities make chemical facility security an issue of national concern.[75] In addition, it must be determined if industry should bear the cost for this initiative or be supplemented in whole or in part by the federal government to ease the economic burden. Industry acceptance of any new initiative will be driven primarily by the source of the funding. The legality issue is of prime importance since the ACC will

[73] Linda Greer, *New Strategies to Protect America: Securing our Nation's Chemical Facilities* (Washington, D.C.:Center for American Progress, 2005), 8.

[74] Dana A. Shea, *Legislative Approaches to Chemical Facility Security* (Washington, D.C.: Congressional Research Service, 2006), 16.

[75] Ibid., 1.

most likely challenge any action that requires the investment of significant resources above what member companies have spent since September 11.

The successful alternative must protect critical infrastructure, address economic feasibility, gain bipartisan political support, have the capacity to be successfully implemented and inspected, and provide a reasonable and communicable metric to determine effectiveness for all criteria. There must be clear evidence that the proposal would safeguard the chemical industry. The cost to implement such safeguards, whether it is target hardening, additional personnel, or inherently safer technology changes must be balanced against the potential to save lives. The ultimate first priority is to save lives but due consideration must be given to protecting the economy and the industry itself.

The DHS, through the American Society of Mechanical Engineers developed the Risk Analysis and Management for Critical Asset Protection (RAMCAP), which is currently being employed in the chemical industry under a pilot program. RAMCAP is an overall strategy and methodology to allow for a more consistent and systematic analysis of the terrorist threat and vulnerabilities against the U.S. infrastructure using a risk-based framework.[76] The sector-specific vulnerability assessment tool being developed is:

- Based upon specific metrics, the use of which is repeatable sector to sector; thereby allowing cross-sector comparative risk assessment.
- Designed to employ specific, defined consequence generators (threat scenarios);
- Designed to evaluate:
  - Consequences (impact produced by the defined consequence generator);
  - Vulnerabilities (potential point targets and/or attack vectors, a broadly accepted surrogate for frequency/probability of success of an attack);

[76] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, Appendix B-5.

- Countermeasures (including factors in mitigation, deterrent factors, detection factors, delay factors, response capability, and inherent robustness);
- Actions/countermeasures at different threat levels;
- Residual security vulnerability (gap analysis).[77]

The alternative must have the potential to gain bipartisan support from federal, state, and local officials. Regardless of the government agency tasked to administer this program, it must have the capacity to be reasonably implemented and audited. The final criterion is the requirement of a metric, understandable to both subject matter experts and the general public that conveys the effectiveness of the effort. The criteria are ranked as listed but the political process may reorder one or more of the items.

B. POLICY OPTION 1: NO FURTHER ACTION

The outcome of the first alternative, no action, is expected to result in large companies with the ability and motivation to adequately safeguard their assets assuming that they agree that the costs of target hardening are necessary. In addition, insurance may be the chosen option if it makes more fiscal sense than the expensive process of target hardening for a rare and unique event such as a terrorist attack. Smaller facilities and those economically challenged will most likely be found to be deficient in their security preparedness efforts. The mechanism to be used to assess this option is New Jersey's Best Practice Standards (Standards) issued on November 21, 2005. The Standards cover 157 chemical facilities and require each site to examine vulnerabilities and hazards that might be exploited by potential terrorists. This information must be available for evaluation by March 21, 2006 and will provide an industry baseline and a framework in which to direct future policy in this area. The no action alternative fails to protect the critical infrastructure, would not satisfy political concerns that regulation is necessary, and would provide no metric to determine effectiveness. In addition, there is no enforcement mechanism beyond association sanctions or expulsion for members who do not meet voluntary standards set by an industry organization. The DHS testified that approximately 20 percent of the facilities DHS classified as high risk do not participate in

[77] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, Appendix B-6.

any voluntary security program.[78] However, since the approach remains voluntary, economic feasibility and program implementation would not be a factor in this scenario.

This policy option would continue the ongoing Chemical Comprehensive Review (CR) undertaken by DHS. The CR is a cooperative government-led analysis of Critical Infrastructure/Key Resource (CI/KR) within the chemical manufacturing sector.[79] The purpose of the CR is to enhance public safety by integrating all levels of government effort to prevent and protect against potential terrorist attack. The CR also represents an all hazards approach as it provides an opportunity to identify and implement best practices that may also apply to other catastrophic events. The program is voluntary and led by the DHS Office of Infrastructure Protection. Additional team members include:

- DHS Risk Management Division which is responsible for the overall coordination of the program and also provides assault planning expertise including physical security and explosive ordnance disposal, and provide technical assistance for buffer zone plans.
- DHS Chemical and Nuclear Protection and Preparedness Division Chemical Sector Specific Agency which is responsible for identifying the regions in which to conduct the CRs.
- DHS Emergency Services Sector responsible to lead workshops to assess emergency planning and preparedness and collect information from stakeholders including plans, strategies, and prior assessments.
- DHS United States Coast Guard which leads maritime security assessment.
- DHS Transportation Security Administration which assesses the security of chemical transport within the region.
- DHS National Cyber Security Division

[78] Robert B. Stephan, *Testimony Before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity of the House Committee on Homeland Security*, Congress No. 109, Session No. 1, June 15, 2005.

[79] Department of Homeland Security, *Fact Sheet, Protecting America's Critical Infrastructure, Chemical Comprehensive Review* (Washington, D.C.: DHS, 2006), 1.

- Federal Bureau of Investigation which participates in law enforcement assessments and supports tactical response planning.[80]

DHS is in the process of conducting CRs on groupings of potentially high-consequence chemical facilities in the following six regions:

- Detroit River, MI
- Los Angeles, CA
- Chicago, IL
- Northern New Jersey
- Lower Delaware River Valley (New Jersey/Delaware/Pennsylvania junction)
- Houston, TX[81]

The three primary components of the CR include Buffer Zone Protection Program Technical Visits, Community Capability Assessment Tool (C-CAT) Workshops, and Emergency Services Capability Assessment (ESCA). The DHS Risk Management Division will provide technical assistance for local law enforcement representatives and emergency responders to complete buffer zone plans for selected chemical facilities.[82] The C-CAT is used by participating community representatives to assess their agency's capabilities. C-CAT is a self assessment of emergency services disciplines that provides an overview of current capabilities that can be used to identify gaps and options for consideration to improve the security around fixed chemical facilities.[83] The final CR component, ESCA, is designed to examine regional capabilities in the event of a terrorist attack. A series of discussions are scheduled to analyze regional capabilities with facility representatives encouraged to provide specific information on necessary response actions.

[80] Department of Homeland Security, *Fact Sheet, Protecting America's Critical Infrastructure, Chemical Comprehensive Review*, 2.

[81] Ibid.

[82] Department of Homeland Security, *How to Prepare for the Chemical Comprehensive Review, A Guide for Emergency Services Organizations* (Washington, D.C.: DHS, 2006), 1.

[83] Department of Homeland Security, *Fact Sheet, The Chemical Comprehensive Review, Community Capability Assessment Tool (C-CAT) Overview* (Washington, D.C.: DHS, 2006), 1.

At the end of these round tables DHS will provide a preliminary review of potential gaps in emergency services planning and preparedness.[84]

C. POLICY OPTION 2: PRESCRIPTIVE REGULATIONS

The second alternative, a mandatory approach through regulation, has the potential to protect the chemical industry and allows the creation of an overall strategy to reasonably implement, oversee, and determine the effectiveness of the program. This dynamic changes depending on the organization charged with this responsibility, but these criteria could be satisfied regardless. However, the alternative has the potential to be prohibitively expensive and would be opposed by those officials supporting a voluntary approach. In addition, the overall cost to the economy must be taken into account through an economic analysis of stricter regulation. Security standards must be implemented with safeguards that protect the private sector from undue burdens that would add little real security but would undermine competition, cost jobs, and make goods and services more expensive.[85]

It is useful to mention the experience of the nuclear industry since the events of September 11 to provide context to the potential of prescriptive regulations to be prohibitively expensive. Security forces at nuclear plants were increased by one-third to approximately 8,000 officers at 103 plants located at 64 sites. Additional security measures included:

- extending and fortifying security perimeters;
- increasing patrols within security zones;
- installing new barriers to protect against vehicle bombs;
- installing additional high-tech surveillance equipment;

---

[84] Department of Homeland Security, *Fact Sheet, Protecting America's Critical Infrastructure, Chemical Comprehensive Review, Emergency Services Capability Assessment* (Washington, D.C.: DHS, 2006), 1.

[85] James Jay Carafano, *Congressional Checklist for Chemical Security* (Washington, D.C.:Heritage Foundation, May 17, 2006), available at: http://www.heritage.org/Research/NationalSecurity/em1000.cfm (Accessed November 8, 2006).

- strengthening coordination of security efforts with local, state, and federal agencies to integrate approaches among the entities.

In total, the nuclear industry has spent 1.2 billion dollars in security-related improvements since September 11.[86] This equates to 18.75 million dollars per site in the last five years. The purpose of this example is not to suggest comparisons between the security needs of the chemical and nuclear industries but rather to demonstrate the potential for significant capital expenditures resulting from prescriptive regulations.

The United States Senate Committee on Homeland Security and Governmental Affairs convened a series of hearings to examine the issue of chemical facility security. At the end of the 109th Congress, the Senate and House of Representatives reached a compromise that led to the Department of Homeland Security being granted the regulatory authority to safeguard chemical facilities. This compromise demonstrates the strong opposition to the implementation of prescriptive regulations similar in nature to those governing the nuclear industry.

D. POLICY OPTION 3: COMBINATION OF A MANDATORY AND VOLUNTARY APPROACH

The final solution has the potential to satisfy all of the criteria if the law and regulations appropriately balance the concerns mentioned above. The targeted companies in this scenario would be those operations found to be non compliant with the ACC's Responsible Care Security Code or alternate methodology that has been determined to be equivalent by the Center for Chemical Process Safety. The political debate will determine if the consensus leads too far to the status quo or to the prescriptive regulatory approach of the second alternative. If bipartisan support can be achieved and a reasonable standard set for cost effectiveness the outcome would be successful.

The recommended solution, as can be seen by the potential for success, is a combination of a voluntary and mandatory approach to safeguarding the chemical industry from terrorist attack. However, as demonstrated in the analysis, the success of

[86] Nuclear Energy Institute, *Post-Sept. 11 Security Enhancements: More Personnel, Patrols, Equipment, Barriers* (Nuclear Energy Institute: Washington, D.C., 2006), available at: http://www.nei.org/index.asp?catnum=2&catid=275 (Accessed February 12, 2007).

this alternative is dependent upon appropriate decision making throughout the process that is consistent with the ranked criteria. If one or more of the criteria is ignored or circumvented the outcome may be no better than that of the status quo of the first alternative or mandatory version of the second alternative.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

The first step in this process is to critically evaluate the chemical industry's compliance with the New Jersey Standards. This research will focus on the chemical facilities located in New Jersey but will be broad enough to be applied at a national level.

The audience is the general public and their elected representatives that live and work within the impact areas of facilities that store and handle extraordinarily hazardous substances and the government officials responsible for regulating the sector and directing policy. Key stakeholders in the process include the chemical industry, environmental groups, and the general public.

Based upon these results the appropriate policy option will be selected and a recommendation satisfying the previously mentioned criteria for success will be formulated. The comments received from the interested parties will be critically analyzed to develop a sound policy proposal for the future. This research will provide a basis for elected officials and government leaders to determine the future policy direction relating to protecting the critical infrastructure of the chemical industry and most importantly the lives of those living in the surrounding area.

Strategy Canvas

A strategy canvas was constructed comparing the voluntary approach which has been in effect since shortly after September 11 with the mandatory approach that DHS is mandated to have in place by April 4, 2007 pursuant to P.L. 109-125. The criteria for the canvas include the ability to protect critical infrastructure, address economic feasibility, gain bipartisan political support, have the capacity to be successfully implemented and inspected, and provide a reasonable and communicable metric to determine effectiveness.

The strategy canvas demonstrated that the regulatory approach was significantly more effective in three areas:

- Protecting critical infrastructure – Based on EPA data there are 14,600 chemical facilities subject to the CAA 112r risk management program requirements. A total of only 1,100 of those facilities are members of an organization that currently has formal security guidelines in effect. Therefore, a voluntary approach results in a significant gap in the number

of facilities of concern that could reasonably be expected to follow appropriate methodology to secure their assets.

- Reasonable and communicable metric - There is no current mechanism and it would be difficult to implement any type of effective metric in a voluntary framework. However, a regulatory approach provides an opportunity to incorporate multiple types of metrics evaluated through an audit and/or inspection program.
- Political support – As can be seen with the recent issuance of P.L. 109-125 and the most recent legislative proposal, the September 29, 2006 amended version of H.R. 5695, there is strong support for a regulatory approach. In addition, based on the recent election results, it is likely that the more prescriptive measures included in H.R. 5695 will gain additional support.

There are two areas of divergence that result from the canvas. These two items are critical as acceptable solutions have the potential to lead to a strategic innovation. These are the two criteria that with the examined business lines favor a voluntary approach:

- Economic feasibility – The majority of economic costs associated with the voluntary approach have already been borne by those facilities that have chosen to institute security enhancements. Any standard regulatory program would create an additional burden to industry with the fear of the extent of such an impact being the prime motivation to object to such an approach.
- Potential for successful implementation - The voluntary approach has been in effect for five years and no additional resource allocations would be necessary to continue forward. The regulatory approach will require resources at the federal and possibly state/local level to establish an effective oversight program.

<u>SWOT Analysis – New Jersey Department of Environmental Protection</u>

Strengths:

- Existing relationship with the chemical industry
- Familiarity with the sites in question

- Experience in rule making, compliance oversight, and enforcement
- Strong community reputation

Weaknesses:

- Unfunded mandate, utilization of existing, limited resources
- Staff expertise is engineering, not security
- Historical focus of command and control
- Additional training required

Opportunities:

- Significant public interest in potential chemical industry risks
- Industry incentive to strengthen security perception
- Legislative support for action
- Standards results provide a baseline for policy recommendations

Threats (Challenges):

- Resistance from strong chemical industry lobby
- Adequate funding source
- Maintaining distinction between environmental and security duties
- Requirements must be practical and economically feasible
- Bipartisan support may prove difficult to achieve

There are five main strategic issues resulting from the SWOT analysis:

1. How does the NJDEP secure the appropriate resources to fund the proposed initiative?
2. What is the best mechanism to solicit stakeholder input and increase the likelihood of bipartisan support?
3. What should be the communicable metric to determine the effectiveness of the selected alternative?
4. What methodology is necessary to ensure that the regulatory requirements are practical and economically feasible?
5. Should inherently safer technology evaluations be part of security regulations or is it more appropriate to address this issue through existing process safety legislation?

THIS PAGE INTENTIONALLY LEFT BLANK

IV. BEST PRACTICE STANDARDS COMPLIANCE STATUS SUMMARY

A. INTRODUCTION

Originally, 157 facilities were notified that they were subject to the Best Practice Standards (Standards) and the New Jersey Department of Environmental Protection (NJDEP) would conduct site inspections at those facilities to verify compliance with the Standards. Since that time, six facilities are no longer subject to the Standards as their operations changed such that they are no longer subject to the Toxic Catastrophe Prevention Act (TCPA) and/or the Discharge Prevention, Containment, and Countermeasure (DPCC) program. The NJDEP completed the Standards inspections in November 2006 with a total of approximately 300 site visits. Follow up inspections were conducted at facilities determined to be non-compliant after the initial audit.

B. SUMMARY OF COMPLIANCE STATUS

Initial compliance inspections were conducted at all of the original 157 facilities. Letters were sent to all of these facilities informing them of whether they had demonstrated compliance with the Standards or whether any deficiencies exist that must be addressed. Initially, ninety-eight (62 percent) of the facilities demonstrated compliance with the Standards. Facilities were given 30 days to satisfactorily resolve any outstanding compliance issues. The most common deficiencies were not conducting a proper security vulnerability assessment utilizing an approved methodology and not affording employees a reasonable opportunity to identify security issues. General compliance with the Standards has been achieved by 144 of the 154 facilities currently subject to the Standards. Follow-up inspections are on going at the remaining 10 facilities to ensure that the noted deficiencies are corrected.

Initially only 42 of the 98 facilities subject to the TCPA regulations reported SIC/NAIC code designations specified in the Standards and were required to conduct an inherently safer technology (IST) evaluation. All 42 of these facilities have documented that they have previously implemented IST or similar risk reduction measures. Thirteen (32 percent) of the facilities have provided a schedule to implement additional IST or

other risk reduction measures, and eight (19 percent) have identified additional IST or risk reduction measures but have not yet scheduled their completion. The remaining twenty (49 percent) facilities had no additional recommendations. It should be noted that these are facilities that have been regulated under the TCPA program for many years resulting in the past implementation of IST and risk reduction measures. Thirty-three (80 percent) of the facilities concluded that at least some of the IST or risk reduction measures identified during their evaluation were infeasible for their operations.

These compliance results clearly indicate that the evaluation of IST is not overly burdensome on industry and is an effective tool for critically evaluating the risk reduction opportunities available at a specific facility. In addition, none of the companies regulated under the Standards brought up concerns about going out of business due to the existence of these additional regulatory requirements for homeland security.

C. NEXT STEPS

It is expected that eventual compliance with the requirements mandated in the Standards will exceed 98 percent. The two percent of facilities that are expected to be deemed out of compliance with all or some portion of the Standards equate to approximately 3 to 5 facilities. The cost of conducting a proper security vulnerability assessment utilizing an approved methodology is likely to be the main reason for prolonged noncompliance. These facilities are limited to those designated in terms of critical infrastructure to be Tier 3. These facilities are non critical infrastructure as defined by the Department of Homeland Security and the New Jersey Office of Homeland Security and Preparedness (OHSP), have no off site consequences in terms of a release, and are generally barely above the TCPA/DPCC regulatory thresholds. If compliance is not achieved in a reasonable time frame, or at least significant progress toward that goal is not demonstrated, the companies in question will be referred to the OHSP for appropriate action.

D. STANDARDS – LESSONS LEARNED

New Jersey embarked into a new area of regulation with the issuance of the Standards in November 2005 and similar to many new initiatives there were many

lessons learned throughout the creation and implementation process. The following outlines those lessons to provide a foundation for recommendations of future action in the area of chemical facility security. These lessons are not ranked in order of significance but simply in the order they appear in the Standards.

Defining the Chemical Sector Universe

The scope of the Standards included those facilities subject to New Jersey's Toxic Catastrophe Prevention Act (TCPA) and Discharge Prevention, Containment and Countermeasure (DPCC) program that reported chemical industry classification codes as their primary business activity. These codes included Standard Industrial Classification (SIC) major groups: 28 (chemical and allied products), 30 (rubber and miscellaneous plastic products), 5169 (chemicals and allied products, not elsewhere classified), or the corresponding North American Industry Classification codes (325, 326, and 424690). The primary purpose of defining the facilities by industry classification was to focus the Standards on the intended target of the chemical industry. The TCPA and DPCC programs regulate many companies in the petroleum, water, wastewater, food, energy, and other industries.

It was evident after implementation of the Standards that the self reporting requirements of the industrial classification system resulted in a universe that included facilities that were not considered part of the chemical sector and also omitted some facilities that were considered critical chemical infrastructure. In addition, there were also cases where two facilities that stored identical amounts of extraordinarily hazardous substances were treated differently simply due to the fact that one reported an industry code that was not included in the scope of the Standards. Although these cases were the minority since the Standards captured the bulk of the expected facilities, future actions must take into account the inherent limitations of the SIC/NAIC system for chemical security applications.

Qualified Security Expert

The Standards required facilities to employ a qualified security expert (who could be an employee of the facility or its parent company) to conduct a security vulnerability

assessment. There was no specific definition of a qualified security expert included within the Standards. This led to numerous determinations by the NJDEP that the individuals tasked to complete the assessments were not qualified or did not have the appropriate background to conduct such an evaluation. Examples included facility employees and outside consultants that were well versed in areas such as chemical process safety and plant management but had little or no security related experience. These situations were resolved either by utilizing corporate security experts or employing an outside security consultant. The cost of consulting services, which were in the range of $20,000 for a small facility, was a significant obstacle for companies with limited resources. In an effort to alleviate this burden, the New Jersey Office of Homeland Security and Preparedness through the 21 county critical infrastructure agencies offered assistance in the evaluation of the security vulnerability assessment. A detailed definition of the necessary qualifications of the individual(s) conducting the assessment is vital to ensure the quality of the final evaluation.

Qualified Process Safety Expert

The Standards required an Inherently Safer Technology evaluation be performed at those facilities subject to the TCPA program. These evaluations were to be conducted by a qualified expert in chemical process safety. Once again there was no specific definition of what constituted a qualified process safety expert. In this case there were only minor problems resulting from a lack of a definition since the facilities already had process safety experts on staff or had hired a consultant in the past to complete process hazard analyses and other risk management program items required by the TCPA program. However, for clarity and ease of implementation, a definition of the necessary qualifications and experience to be considered a process safety expert is recommended to be included in any future regulation.

Inspection of Evaluations

The Standards required that all assessments, plans, reports, and reviews required by the Standards be maintained on site for evaluation by representatives of NJDEP or the Task Force during normal business hours. The premise for retaining the information on

site instead of submitting the information to the NJDEP was the concern regarding the ability of the NJDEP to adequately protect the information. The concerns included adequate protocol and safeguard mechanisms at the NJDEP offices and protection from New Jersey's Open Public Records Act. The industry concerns were not without merit but the efficiency of the inspection process was definitely hampered by this requirement. Additional NJDEP and industry resources were required as additional site visits were necessary for follow up visits that could have been completed through submissions and evaluations in the office. Detailed handling and storage protocol and legislative protection from public information requests must be implemented to permit sensitive information to be submitted to the public agency charged with the responsibility for chemical facility security.

A related issued, not specifically mentioned in the Standards, is the background check or lack thereof of the government employees that have access to the sensitive documents. The NJDEP staff are not required to have any type of background check to perform these types of inspections nor is it mandated that they be U.S. citizens. This issue was brought up by a number of facilities that require detailed background checks of their own employees before they are hired or at minimum before they can access or handle sensitive information. The strongest objections came from facilities that were also subject to the Maritime Transportation Security Act which prohibits the release of any sensitive security information to any individual that has not undergone a prescribed background evaluation. In the case of the Coast Guard these issues were resolved through the Sensitive Security Information non disclosure forms which were executed by NJDEP staff. Future consideration should be given to administering adequate background checks for all government employees that are required as part of the job responsibilities to access, evaluate, or process security related information.

On December 19, 2006, New Jersey Governor Jon S. Corzine signed a Senate Committee substitute for Senate Bill Nos. 462 and 1289 which requires independent contractors to submit to background checks to work within facilities subject to the NJTCPA program. The Department of Law and Public Safety is required to perform criminal history record background checks on applicants employed by or to be employed by independent contractors determined to working in a critical position. At a minimum,

these checks include a credit investigation, a Social Security number verification to detect informational inconsistencies, and a cross-referencing of all applicants against appropriate law enforcement advisories and terror watch lists. This act takes effect 270 days after enactment, except that the Attorney General, Director of the Office of Homeland Security and Preparedness, and the Commissioner of Environmental Protection may, prior to the effective date, take such anticipatory action as shall be necessary for the implementation of this act.

These lessons learned should not be seen as a failure of the overall Standards initiative but rather unforeseen consequences that can be used to improve any similar programs in the future. The Standards compliance results were very positive and industry preparedness and willingness to correct outstanding deficiencies exceeded the expectations of many of the stakeholders involved in the process. The voluntary approach for chemical security and the term cooperative seemingly go hand in hand in most security discussions. However, the Standards were a mandatory requirement and the industry cooperation, in most cases, was positive and unchanged from that of the previous voluntary Best Practices.

V. CONCLUSIONS/RECOMMENDATIONS

A. INTRODUCTION

The conclusions of this research and the recommendations to address chemical facility security focus on the appropriate legislative approach, responsible government agency, scope of the chemical universe, public preparation, and inherently safer technology. There are also many other suggestions included within these topics.

B. LEGISLATIVE APPROACH

The suggested policy direction resembles a standard regulatory approach but would be modified to address the economic and implementation issues associated with a typical command and control structure. The economic impacts have the potential to be mitigated by rewarding those facilities that have voluntarily adequately protected their assets. These rewards could be in the form of recognition, less government oversight (tiering the regulations), and auditing the facilities versus the standard inspection and enforcement visits. The proposal to audit is in the context of compliance assistance instead of administrative and criminal penalties that result from enforcement inspections. Economic impacts to smaller facilities without the financial ability to invest substantial resources can potentially be reduced by tiering requirements based upon the risk associated with a particular site. Tax incentives and grant or low interest loans are also an option for consideration.

The Standards demonstrated that significant investment by the chemical industry, estimated to be 100 million dollars in New Jersey alone, for security enhancements have been made since September 11. These voluntary efforts should be appropriately recognized in the regulations. Initial baseline evaluations of the universe to determine compliance will permit such recognition and allow facilities to be classified as compliant. Therefore, the onus on facilities that have truly made adequate efforts to safeguard their assets will be limited to demonstrating such actions through documentation and participation in a site audit. It is important to note that significant monetary investment does not in and of itself guarantee full compliance with risk-based standards as it is unknown if such enhancements were appropriately targeted.

Government oversight should be prioritized by the risk posed and the vulnerabilities determined to exist at the facility. Companies adhering to industry best practices and satisfactorily resolving outstanding deficiencies would require less initial oversight and qualify for a more conservative audit frequency schedule in the future. Assuming there are no major changes at the facility that would require reevaluation of the vulnerability assessment or other security protocol revisions, the responsible agency can then divert limited resources to those facilities that are determined to be non-compliant with the regulations. The type of oversight, audit versus inspection, is also a critical component of this proposal. 6 CFR 27.240(a)3 stipulates that the DHS will not disapprove a Site Security Plan based on the presence or absence of a particular security measure. Audit visits focused on compliance assistance will leverage the public and private sector expertise and permit the facility to implement the measures determined to be most effective at that particular site to attain compliance with the standards. Inspections combined with the threat of administrative and criminal penalties are generally less effective and have the potential to result in enhancements that meet the letter of the rule but are not the best solution to a specific deficiency. However, the audit methodology if unsuccessful would lead to a traditional enforcement response through mandatory penalties to attain compliance.

Economic impacts, especially for smaller facilities, must be taken into consideration. In general, these facilities pose less risk due to a catastrophic release and shouldn't be held to the same standard as a company that would impact a significant number of people. However, the cost of conducting even a security vulnerability analysis, even if no further actions are deemed necessary, can be a significant obstacle to a company. Compliance assistance, grants, tax incentives, and low interest loans are possible alternatives to alleviate this burden. A mechanism would be required to be built into the regulations, possibly based on the size of the company or gross revenue to determine applicability of such assistance.

C. RESPONSIBLE AGENCY

The Department of Homeland Security (DHS), consistent with P.L. 109-125, is the governmental agency best suited to undertake the responsibility for the promulgation

and implementation of chemical security requirements. In consideration of the lack of chemical process safety expertise within DHS and limited historical knowledge of the CAA 112r sites, a close partnership with the Environmental Protection Agency (EPA) is required to address gaps and overlaps between security and process safety.

The proposal is centered on delegating oversight responsibility to the state level. DHS is not currently staffed to evaluate 14,600 facilities and it is not realistic that any one agency could effectively handle such a universe. DHS would still be the responsible regulatory agency but would delegate the responsibility, similar to how EPA has handled air and water regulations and states obtaining Agreement State status from the Nuclear Regulatory Commission. In the case of the former, many states have an overarching Performance Partnership Agreement with EPA which guides the efficient administration of both Federal and State resources toward the common goal of environmental protection. This approach may serve as a model for delegated homeland security programs. The specific state agency tasked with this responsibility is likely to vary depending on the existing and potential capabilities of the current State homeland security and environmental protection agencies. It is also likely that a number of states may not be interested or have the resources to assume a delegation status. In those cases, DHS would retain sole regulatory control for the purposes of homeland security of the chemical facilities of concern located in that jurisdiction.

The Advance Notice of Rulemaking, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards defines a "covered facility" to be a chemical facility determined by the Assistant Secretary to present high levels of security risk, or a facility that the Assistant Secretary has determined is presumptively high risk under Section 27.200.[87] Although there are multiple criteria that could potentially justify a determination of high risk, the first Top-screen question is whether the toxic release worst-case scenario as identified under the EPA Risk Management Program might expose a residential population greater than or equal to 200,000 persons. The second question is whether a flammable release worst-case scenario might expose a residential population greater than or equal to 1,000 persons. In the case of New Jersey, this consequence threshold would result in approximately 13 percent of the facilities subject to the NJTCPA program

potentially being a covered facility pursuant to 6 CFR Part 27. It is logical that the DHS would set the regulation threshold at a very high level considering the vast number of chemical facilities throughout the country. However, it is difficult to justify 87 percent of the universe being exempt from 6 CFR Part 27 considering that the majority of those facilities do have significant off site consequences even though they are less than 200,000 and 1,000 persons for a toxic and flammable release, respectively. Consideration should be given to reducing the toxic consequence to 20,000 persons to appropriately capture facilities that present a high level of security risk.

The completion of the Top-screen should not be a one time process since facilities routinely change the amount and type of substances being stored and handled. A requirement to update the Top-screen based upon submission of an updated RMP would ensure that the universe of covered facilities is accurate. However, since RMPs are required to be updated for various reasons that would not affect the Top-screen, changes should be limited to those that increase or decrease the amount of extraordinarily hazardous substances on site, modify the off-site consequence analysis, or otherwise impact preparedness and response activities.

Delegation will require the regulations to address an appropriate resource mechanism to provide the State agency in question adequate funding to implement an oversight program. This could be accomplished through direct funding from the DHS, a fee based program assessing the companies in question based upon risk, or a combination thereof. States such as New Jersey that have delegation status for the EPA Risk Management Program already have established fee structures in place for this universe of facilities which could be adjusted to account for the additional costs associated with administering chemical security standards.

The question of Federal preemption will turn either on the application of implied preemption, or on the nature of any express preemption in 6 CFR Part 27.[88] The principle of implied preemption is centered on the fact that no state or local authority can frustrate the purposes of a Federal law or regulatory program. A state or local regulation

[87] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, 73.

[88] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, 66.

may be preempted, for example, where that regulation conflicts with an activity or plan specifically approved under Federal law.[89] Section 27.405 provides for the review and preemption of State laws and regulations by the Assistant Secretary. The DHS will review State laws, administrative actions, or decisions or orders of a court under State law and regulations submitted under this section, and will opine whether –

(A) complying with the State law or regulation and a requirement of this Part is not possible; or

(B) the application or enforcement of the State law or regulation would present an obstacle to or frustrate the purposes of this Part.[90]

An evaluation of the proposed preemption language by the Congressional Research Service determined that the proposed rule seems to imply that any state regulation that does require a specific security measure would be preempted. If this proposed language is retained in the interim final rule, it seems likely that any existing state regulations, such as those in New Jersey, would be preempted by the performance-based federal regulation.[91]

It is imperative that States retain the ability to be more restrictive as appropriate to ensure that preparedness is measured in line with potential vulnerabilities. A one size fits all standard is not practical across our diverse nation. A minimum standard set by DHS will ensure a level playing field for the chemical industry with the understanding that jurisdictions with unique vulnerabilities have the ability to implement stricter standards to adequately safeguard their citizens.

States, such as New Jersey, have taken critical steps to address chemical facility security well over three years ago. It is recognized that most states have not taken similar action and therefore, federal regulations to create minimum national chemical facility standards is essential. At the same time, it is also important not to penalize those pro-active states and allow the states to retain the authority to adopt enhanced security requirements if states determine they are necessary. No two states are alike, and the risks

---

[89] Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*, 67.

[90] Ibid., 106.

[91] Dana A. Shea and Todd B. Tatelman, *Chemical Facility Security: Regulation and Issues for Congress* (Washington, D.C.: Congressional Research Service, 2007), 7.

posed by every facility present unique challenges based on location, population size, and other factors. Federal standards must be a floor ensuring a base level of protection, not a ceiling that constrains a State's ability to protect its citizens.

D. SCOPE OF UNIVERSE

The chemical facilities subject to the EPA 112r requirements is a logical starting point in defining the universe of facilities subject to mandatory security requirements. However, the off site consequences of the 14,600 facilities storing extraordinarily hazardous substance vary significantly which demonstrate the need for a tiered regulatory approach. A facility with the potential to impact a large metropolitan population should not be held to the same standard as one that would have no or limited off site consequences in the event of an accident or intentional attack.

There are a number of EPA RMP facilities exempt from the proposed 6 CFR Part 27 Chemical Facility Anti-Terrorism Standards. Pursuant to Section 550, the regulations will not apply to public water systems (as defined by section 1401 of the Safe Drinking Water Act) and water treatment works facilities (as defined by section 212 of the Federal Water Pollution Control Act). Exempting public water systems and treatment works is not appropriate as these facilities many times pose a higher risk than sites currently captured under the DHS definition of a covered facility. Unlike the mandatory programs in place at the exempted Nuclear Regulatory Commission and the Maritime Transportation Security Act (MTSA) facilities, the water and wastewater industries are only subject to voluntary standards which cannot be considered equivalent to that proposed under 6 CFR Part 27. Since an equivalent security program is not in place for the water and wastewater industries, these facilities should not be exempt from the requirements of 6 CFR Part 27. Facilities that present a high level of security risk should be subject to federal regulations, regardless of the industry in question, unless it can be demonstrated that equivalent mandatory requirements are already established.

A three tier proposal, defined as follows, would serve to address the degree of variation in the risk and consequence inherent within the chemical sector.

- Tier 1 – Facilities that meet the covered facility definition currently proposed in 6 CFR Part 27.

- Tier 2 – Facilities that have EPA off site consequences but are not considered to be high risk facilities as defined by the DHS.
- Tier 3 – Facilities that are subject to the EPA Risk Management Program but their worst case scenario does not result in any off site consequences.

Tier 1 facilities would face the most stringent standards in terms of risk-based performance standards. Criteria similar to that proposed in 6 CFR Part 27.230 would be appropriate for these facilities. Part 27.230 requires each covered facility to select, develop, and implement measures designed to:

1. secure and monitor the perimeter of the facility;
2. secure and monitor restricted areas or potentially critical targets within the facility;
3. control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter;
4. deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;
5. secure and monitor the shipping and receipt of hazardous materials for the facility;
6. deter theft or diversion of potentially dangerous chemicals;
7. deter insider sabotage;
8. deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, Supervisory Control And Data Acquisition (SCADA) systems, and other sensitive computerized systems;
9. develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;
10. maintain effective monitoring, communications and warning systems;

11. ensure proper security training, exercises, and drills of facility personnel;
12. perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or potentially critical targets;
13. escalate the level of protective measures for periods of elevated threat;
14. address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;
15. report significant security incidents to the Department;
16. identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;
17. establish official(s) and an organization responsible for security and for compliance with these standards;
18. maintain appropriate records; and
19. address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;
20. address any additional performance standards the Assistant Secretary may specify.[92]

Tier 2 facilities are defined as those facilities that have off-site consequences but are not considered to be high risk facilities pursuant to the DHS definition. These facilities, although of less magnitude than the Tier 1 sites, have a significant potential for off-site impacts. It is proposed that these sites be required to follow the same risk-based performance standards with the understanding that the implementation measures would not be required to be as robust as those of the high risk facilities. It would be necessary to develop criteria of acceptable measures for Tier 2 sites. A general example could be screening and/or inspecting individuals and vehicles as they enter the site. An acceptable

[92] Shea and Tatelman, *Chemical Facility Security: Regulation and Issues for Congress*, 87.

Tier 1 approach would be inspecting personal identification and the vehicle itself while a Tier 2 site would be considered to be compliant with only protocol in place for individual inspection.

Tier 3 sites are subject to the EPA Risk Management Program but do not have any off-site consequences. The risk-based performance standards for this tier would focus on training, exercising, and background checks. Although controlling access and methods to deter threats are not emphasized for this tier, such measures could be required based upon the results of the security vulnerability analysis. Following the previous example for the Tier 1 facilities, the modified Tier 3 standards may include:

1. develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;
2. maintain effective monitoring, communications and warning systems;
3. ensure proper security training, exercises, and drills of facility personnel;
4. perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or potentially critical targets;
5. escalate the level of protective measures for periods of elevated threat;
6. address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;
7. report significant security incidents to the Department;
8. identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;
9. establish official(s) and an organization responsible for security and for compliance with these standards;
10. maintain appropriate records; and

11. address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;

12. address any additional performance standards the Assistant Secretary may specify.

E. PUBLIC PREPARATION

Determination of the appropriate role and responsibility of government and the chemical industry in preparing the public for a terrorist attack against critical chemical sector infrastructure is important to the success of any regulatory initiative. The implementation of effective preparedness and response protocols are critical to avoid confusion and panic, a primary goal of most terrorist organizations. Historically, the response plans in place at chemical facilities are a collaborative effort between the private sector, government agencies, and the local emergency response organizations. In general, the public has played no active role in this process or participates in the annual drills to exercise the plans. An incident of such magnitude that the vulnerability exceeds over 1,000,000 people will quickly exceed the capabilities of dedicated response resources. Therefore, it is necessary engage the public in the planning process to reduce the threat of panic, confusion, and distrust of government direction to shelter in place or evacuate. Research on population responses to a wide range of natural and technological disasters suggests that there is a tendency toward adaptability and cooperation.[93] In addition, nonprofessionals in the immediate vicinity have saved the majority of people rescued in disasters, greatly aiding the work of the professionals who respond.[94]

In order to minimize disruption of daily routines and promote community cohesion it is necessary to adequately communicate the worst case scenarios that may result from a terrorist attack on a local chemical facility. The evaluation of worst case scenarios is required by EPA under the Clean Air Act Section 112r. Based upon the largest vessel on site releasing its entire contents within 10 minutes, a plume model is developed specific to the hazardous substance in question to generate an estimated

[93] Thomas A. Glass and Monica Schoch-Spana, "Bioterrorism and the People: How to Vaccinate a City against Panic," *Confronting Biological Weapons* (Baltimore, MD: Infectious Diseases Society of America, January 15, 2002).

[94] Ibid.

population amount in the vulnerability zone. These off site consequence analyses are not available to the public but can be viewed under certain conditions through EPA reading rooms. Access restrictions are logical as this information is sensitive and would be a valuable planning tool to a terrorist organization. However, the lack of this information in the public domain can have serious implications in any response scenario. The recommended action protocol can vary greatly depending on the specific hazardous substance of concern.

Timely and consistent communication of information regarding the prevention of terrorist attacks may help alleviate fear and anxiety and provide confidence in the government's ability to protect the public.[95] Limited information on the types of chemical threats in their neighborhood and the appropriate responses to safeguard yourself and loved ones will intensify fear and anxiety within the community. Results revealed that those experiencing more anger had more optimistic beliefs and those experiencing fear had more pessimistic beliefs about risks from both terror and non terror related events.[96] The goal should be to provide sufficient information that educates populations about expectable responses and coping strategies to increase community resilience. It is important to note that an appropriate balance must be struck to ensure that the information is provided in such a context to not divulge unnecessarily any sensitive data that could be used for malicious purposes.

The lack of transparency of certain aspects of government regulatory oversight of the chemical industry has led to distrust of the industry in general and particularly the private sector motivation to adequately protect the surrounding community from a catastrophic release of a hazardous substance. The protection of sensitive information, arguably a necessity in consideration of the threat of terrorism, has added to the perception that the first priority of industry is to maximize profit and minimize security enhancements that require significant investment.

Communicable industry metrics are necessary to alleviate concerns that industry is not proactively and effectively addressing security issues and that appropriate

[95] National Academy of Sciences, *Developing Strategies for Minimizing the Psychological Consequences of Terrorism Through Prevention, Intervention, and Health Promotion* (Washington, D.C.: The National Academies Press, 2003), 118, available at: http://books.nap.edu/catalog/10717.html (Accessed December 11, 2006).

[96] Ibid., 119.

government agencies are actively involved in the oversight of these initiatives. Open communication channels with community leaders will not only have a positive effect on increasing knowledge and trust but will also increase the effectiveness of future regulatory proposals addressing chemical industry security.

The chemical industry, from a process safety standpoint, is heavily regulated by various Federal and state agencies. As a result, all facilities of concern have detailed emergency response plans in place and are required to annually exercise these plans. Originally, these plans considered only accidental releases but incorporating terrorism aspects did not require significant resources as the response actions are very similar. However, strong public opinion that greater effort is necessary to adequately protect the chemical infrastructure from terrorism has led to P.L. 109-125 which requires DHS to promulgate chemical security standards no later than April 4, 2007. Professionals have made the argument that public risk perceptions are irrational but regardless there is a benefit to take appropriate regulatory action. In a democracy, interventions that address misguided fears of a majority, or at least a large number of citizens, are legitimate even if only anxiety is reduced and objective threat reduction is negligible.[97]

Risk perceptions and many other judgments are guided by heuristics, implicit and intuitive shortcuts, which often contrast dramatically with the logical, probability-based analytical process employed by professional experts.[98] However, the public is at a distinct disadvantage as the majority of the information necessary to make a reasonable risk assessment in regards to the chemical industry is not in the public domain. Off site consequences and the results of various plume models are only available through EPA reading rooms and the inputs to those models are not always provided. In addition, the complexity of the modeling and the underlying assumptions are many times difficult for the average individual to comprehend. In many cases the only exposure to vulnerability analyses of the chemical industry is through media accounts which very often provide

[97] C.R. Sunstein, "Terrorism and Probability Neglect," *Journal of Risk and Uncertainty*, 26(2/3), (2003): 121-136.

[98] James M. Breckenridge and Philip G. Zimbardo, *Psychology of Terrorism* (New York: Oxford University Press, 2007), 121.

inaccurate or at least information out of context which serves to increase fear, anxiety, and distrust with the private sector and government agencies charged with regulatory oversight.

Access to accurate information, the ability to have an active role in preparedness exercises, and understanding the potential response actions are all vital to public trust, support for government policy, and minimizing loss of life due to an actual terrorist event. There are obviously limitations on the type of information and the detail of such that can be shared with the public, the role that members of the public can play during exercises, and the fact that a true catastrophic event will result in casualties. The following three steps are recommended to provide the public with realistic risk information, an active role in preparedness activities, and an understanding of their role and responsibilities should an attack occur in their neighborhood. Public participation in dealing with community disasters has repeatedly been shown to bolster public morale and ameliorate psychological stress – from the bombings in London during World War II to the modern day Israeli/Palestinian conflict.[99]

1. Information Sharing

Public forums for interested citizens living in EPA RMP vulnerability zones would provide a reasonable baseline understanding of the potential impacts of a chemical release, whether accidental or intentional, on their community. It may not be practical to conduct these forums for each chemical facility as industrialized areas many times are located within the vulnerability zones of multiple chemical facilities. County wide forums may be the most logical approach as this is consistent with emergency response organization structures outside of large metropolitan areas. The forums could be chaired by appropriate local government officials with participation by the affected chemical companies. The forum should provide a general understanding of the facilities in the area, the hazardous substances of concern, and the plans in place to respond in the event of an incident. An open dialogue with questions from the public will allow the government officials to appropriately focus the meeting on the specific concerns of the community. Educating the public and addressing their concerns to the maximum extent

[99] Susan E. Brandon and Andrew P. Silke, *Psychology of Terrorism* (New York: Oxford University Press, 2007), 187.

possible will serve to empower the community and provide a sense of control over their own destiny should such a catastrophe occur. Alleviating the fear of the unknown and a sense of helplessness surrounding an act of terrorism will greatly benefit existing preparedness initiatives.

2. Public Preparedness Role

In general, chemical industry emergency response exercises do not have active participation from the local community, except for the emergency responders in the area. This void is important as there is no metric to determine if the communication channels are truly effective and that the message is being understood and appropriately implemented. It is obviously not practical to have full scale notifications or mock evacuations during each drill but a representative sample of individuals will provide a valuable benchmark. Communication methods such as reverse 911, siren activations, media broadcasts, and other alert mechanisms can be improved with public involvement focused on deficiencies of the existing protocol and areas of the community that are not being reached. This change can be implemented through regulatory amendments that add public representation to the various agencies that are currently required to play a role in the annual response exercises.

3. Potential Response Actions

The determination of the appropriate recommended protective actions in the event of a hazardous chemical release is not only dependent upon the amount, duration, and weather conditions but also the substance in question. Therefore, the public needs to be well aware of the types of substances that they could be exposed to and the range of protective actions that may be recommended by government officials. In many cases, not adhering to the specific government direction potentially results in putting yourself in harms way. An example would be the tracking of a release plume. The plume will probably cover approximately one-sixth of the vulnerability zone and those individuals may be directed to evacuate. The remaining population would be directed to shelter in place but if they choose to evacuate anyway it very well could be into the direction of the plume or at least hinder those individuals that were appropriately ordered to evacuate. Therefore, if the community understands the decision making process that results in

protective action recommendations individuals would be more likely to respond appropriately. Providing the large picture with the facts necessary to understand how an event is likely to unfold and educating the community on their roles and responsibilities will strengthen cohesion and resilience in the vulnerability zone.

As can be seen, these recommendations are very broad and there will be many obstacles to overcome at the detail level prior to implementation. However, it is clear that the best laid chemical industry preparedness and response plans are less effective without incorporating the public into the process. Building trust and confidence in government policy is vital to reducing the fear and anxiety inherent to acts of terrorism. There is no expectation that planning, capital investments, and response resources can eliminate the potential for terrorism but reactions of anger and optimism instead of fear and pessimism are within our reach.

F. INHERENTLY SAFER TECHNOLOGY

The implementation of Inherently Safer Technology (IST) has clearly led to increased process safety and reduced risk throughout the chemical industry. It is important to understand the distinction between the evaluation of IST alternatives and the requirement of implementation of such alternatives in terms of government regulation. The New Jersey Standards, for example, required only the evaluation of potential alternatives and did not require implementation, only justification from the owner as to why implementation was not practical at that their site. Mandatory implementation is not feasible in an industry that is so diverse in terms materials and products, and so complex in terms of chemistry and operations. However, the evaluation of IST, as was demonstrated in New Jersey is not a significant hardship for the chemical industry.

The significant difference with IST is that it is primarily a process safety function which does have ancillary homeland security benefits. However, it is not appropriate or effective to include IST within chemical security standards. There are overlaps between security and process safety but the training and experience necessary to become skilled in these areas is quite different. Therefore, it is recommended that future IST regulatory efforts be guided and implemented by the EPA and those States delegated the

responsibility for implementation of the Clean Air Act Section 112r. It would be necessary to ensure that there is nothing in an IST regulation that would frustrate the purposes of 6 CFR Part 27.

It is proposed that IST evaluation be required for all facilities subject to the EPA Risk Management Program. Similar to the New Jersey Standards, companies would be required to evaluate IST alternatives across their entire operations. IST is defined as the principles or techniques incorporated in a covered process to minimize or eliminate the potential for an EHS accident that include, but are not limited to, the following: 1) reducing the amount of EHS material that may be released; 2) substituting less hazardous materials; 3) using EHSs in the least hazardous process conditions or form; 4) designing equipment and processes to minimize the potential for equipment failure and human error. This review must also include an analysis of whether the adoption of IST alternatives is practicable and the basis for any determination that implementation of IST is impractical.

In addition to specific items that must be taken into consideration as part of an IST evaluation, reasonable criteria must be established to determine practicality. This is difficult to prescribe in a regulatory structure but is imperative to ensure that all sites are held to a similar standard. Anticipated reasons for a determination that an alternative is impractical may include cost, efficiency, product quality, and similar negative effects on the current business activity. An appeal mechanism would also be necessary to provide owners an avenue to contest a determination that the basis for an impractical decision is not acceptable.

The background and experience to be considered a process safety expert and qualified to conduct the IST evaluation must be defined by regulation. These individuals could be employed by the site, corporate staff, or independent consultants but must have the ability to demonstrate proficiency in this area. It is very possible that the same individuals that completed the process hazard analyses and other risk management program items will similarly meet the qualifications to conduct and IST evaluation.

The results of the New Jersey Standards demonstrated the positive effects of simply evaluating IST alternatives. There are a number of facilities that evaluate IST as part of their standard operating procedures and would therefore not be significantly

impacted by regulatory requirements. The largest benefit from IST requirements is driving those companies that have not historically considered process safety alternatives to institute a continuous improvement culture within the organization.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Andress, Carol. *Testimony Before the Senate Homeland Security and Governmental Affairs Committee*. Congress No. 109, Session No. 1. July 13, 2005.

Australian Government Attorney's General Department – CI Owners and Operators. *Trusted Information Sharing Networks for Critical Infrastructure Protection.* Canberra: Attorney General of Australia, 2005. Available at: http://www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/RWP2D0BFCB21BFFDE9BCA2571710012CC9EC. [Accessed October 25, 2006].

Bandy, Stephen P. *Testimony Before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity of the House Committee on Homeland Security*. Congress No. 109, Session No. 1. June 15, 2005.

Bollinger, Robert E., David G. Clark, Arthur M. Dowell III, Rodger M. Ewbank, Dennis C. Hendershot, William K. Lutz, Steven I. Meszaros, Donald E. Park, and Everett D. Wixom. *Inherently Safer Chemical Processes, A Life Cycle Approach*. New York, New York: American Institute of Chemical Engineers, 1996.

Bone, Craig E. *Testimony Before the Senate Homeland Security and Governmental Affairs Committee*. Congress No. 109, Session No. 1. July 27, 2005.

Bozarth, Hal. *Testimony Before the New Jersey Department of Environmental Protection in the matter of Chemical Security Best Practices.* Trenton, NJ, December 1, 2005.

Brandon, Susan E. and Andrew P. Silke. *Psychology of Terrorism*. New York: Oxford University Press, 2007.

Breckenridge, James N. and Philip G. Zimbardo. *Psychology of Terrorism*. New York: Oxford University Press, 2007.

Cilluffo, Frank J. *Testimony Before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Committee on Homeland Security*. Congress No. 109, Session No.1. June 15, 2005.

Carafano, James Jay. *Principles for Congressional Action on Chemical Security*. Washington, D.C.: Heritage Foundation, 2006. Available at: http://www.heritage.org/Research/HomelandDefense/em997.cfm [Accessed November 8, 2006].

_____. *Congressional Checklist for Chemical Security*. Washington, D.C.: Heritage Foundation, 2006. Available at: http://www.heritage.org/Research/NationalSecurity/em1000.cfm [Accessed November 8, 2006].

Commission of the European Communities. *Communication from the Commission on a European Programme for Critical Infrastructure Protection.* Brussels: Commission of the European Communities, 2006.

_____. *Green Paper on a European Programme for Critical Infrastructure Protection.* Brussels: Commission of the European Communities, 2005.

_____.*Proposal for a Directive of the Council on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection.* Brussels: Commission of the European Communities, 2006.

Committee on Assessing Vulnerabilities Related to the Nation's Chemical Infrastructure, National Research Council. *Terrorism and the Chemical Infrastructure: Protecting and Reducing Vulnerabilities.* Washington, D.C.: The National Academies Press, 2006. Available at: http://www.nap.edu/catalog/11597.html [Accessed December 1, 2006].

Conrad, Jamie. *Testimony Before the New Jersey Department of Environmental Protection in the matter of Chemical Security Best Practices.* Trenton, NJ, December 1, 2005.

Datz, Todd. "Capital Ideas." *CSO Magazine*. December 1, 2003. Available at: http://www.csoonline.com/read/120103/ideas.html [Accessed October 17, 2005].

Department of Homeland Security, Office of Intelligence and Analysis/Office of Infrastructure Protection, Homeland Infrastructure Threat & Risk Analysis Center (HITRAC). *Strategic Sector Assessment (U//FOUO) Chemical Sector*. Washington, D.C.: DHS, 2006. FOUO

Department of Homeland Security, *DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, Chemical Facility Anti-Terrorism Standards*. Washington, D.C.: DHS, 2006.

_____. *Fact Sheet, Protecting America's Critical Infrastructure, Chemical Comprehensive Review*. Washington, D.C.: DHS, 2006.

_____. *Fact Sheet, Protecting America's Critical Infrastructure, Chemical Comprehensive Review, Emergency Services Capability Assessment.* Washington, D.C.: DHS, 2006.

_____.*Fact Sheet, The Chemical Comprehensive Review, Community Capability Assessment Tool (C-CAT) Overview*. Washington, D.C.: DHS, 2006.

_____.*How to Prepare for the Chemical Comprehensive Review, A Guide for Emergency Services Organizations*. Washington, D.C.: DHS, 2006.

DePasquale, Sal. *Testimony Before the House Committee on Homeland Security Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity*. Congress No. 109, Session No. 1. June 15, 2005.

Dunn, Myriam. "The Socio-political Dimensions of Critical Information Infrastructure Protection (CIIP)." *Int. J. Critical Infrastructures* Vol. 1, Nos. 2/3 (2005): 260.

Durbin, Martin J. *Testimony Before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the House Committee on Homeland Security*. Congress No. 109, Session No. 1. June 15, 2005.

_____. *Testimony Before the Senate Homeland Security and Governmental Affairs Committee*. Congress No. 109, Session No. 1. July 13, 2005.

Falkenrath, Richard A. *Testimony Before the United States Senate Committee on Homeland Security and Governmental Affairs*. Congress No. 109, Session No.1. April 27, 2005.

George Mason University School of Law Critical Infrastructure Protection Program. "Trust, The Critical Ingredient in Australia's Critical Infrastructure Protection Strategy." *The CIP Report* Volume 4, No. 12 (June 2006): 3-4.

_____. *Critical Infrastructure Protection in Canada*. Volume 4, No. 12 (June 2006): 2 and 16.

Glass, Thomas A. and Monica Schoch-Spana. "Bioterrorism and the People: How to Vaccinate a City Against Panic." *Confronting Biological Weapons*. Baltimore, MD: Infectious Diseases Society of America, 2002.

Government Accountability Office. *Protection of Chemical and Water Infrastructure*. Washington, D.C.: GAO, 2005. Available at: http://www.gao.gov/htect/d05327.html [Accessed October 17, 2005].

Greer, Linda. *New Strategies to Protect America: Securing our Nation's Chemical Facilities*. Washington, D.C.: Center for American Progress, 2005.

House of Representatives. *Committee Reports, House Homeland Security, House Report 109-707, Part 1 – To accompany H.R. 5695*. Washington, D.C.: September 29, 2006.

Leta, Suzanne. *Testimony Before the New Jersey Department of Environmental Protection in the matter of Chemical Security Best Practices*. Trenton, NJ, December 1, 2005.

Miller, Clyde. *Testimony Before the New Jersey Department of Environmental Protection in the matter of Chemical Security Best Practices*. Trenton, NJ, December 1, 2005.

National Academy of Sciences. *Developing Strategies for Minimizing the Psychological Consequences of Terrorism Through Prevention, Intervention, and Health Promotion*. Washington, D.C.: The National Academies Press, 2003. Available at: http://books.nap.edu/catalog/10717.html [Accessed December 11, 2006].

Nuclear Energy Institute. *Post-Sept. 11 Security Enhancements: More Personnel, Patrols, Equipment, Barriers*. Washington, D.C.: Nuclear Energy Institute, 2006. Available at: http://www.nei.org/index.asp?catnum=2&catid=275 [Accessed February 12, 2007].

Office of Homeland Security. *National Strategy for Homeland Security.* Washington, D.C.: Government Printing Office, 2002.

Poje, Gerald. *Testimony Before the Senate Homeland Security and Governmental Affairs Committee*. Congress No. 109, Session No. 1. July 13, 2005.

Public Safety and Emergency Preparedness Canada. *Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection*. Ottawa: Government of Canada, 2004. Available at: http://www.psepc.gc.ca/prg/em/nciap/position-paper-en.asp [October 14, 2006].

_____. *Joint Infrastructure Interdependencies Program*, Ottawa: Government of Canada, 2004. Available at: http://www.psepc.gc.ca/prg/em/jiirp/index-en.asp [October 14, 2006].

Renner, Paul. *Testimony Before the New Jersey Department of Environmental Protection in the matter of Chemical Security Best Practices*. Trenton, NJ, December 1, 2005.

Schierow, Linda-Jo. *Chemical Plant Security.* Washington, D.C.: Congressional Research Service, 2005.

Shea, Dana A. *Legislative Approaches to Chemical Facility Security.* Washington, D.C.: Congressional Research Service, 2006.

Shea, Dana A. and Todd B. Tatelman. *Chemical Facility Security: Regulation and Issues for Congress.* Washington, D.C.: Congressional Research Service, 2007.

Stephan, Robert B. *Testimony Before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity of the House Committee on Homeland Security*. Congress No. 109, Session No. 1. June 15, 2005.

_____. *Testimony Before the Senate Homeland Security and Governmental Affairs Committee*. Congress No. 109, Session No. 1. June 15, 2005.

Stephenson, John B. *Testimony Before the Senate Committee on Homeland Security and Governmental Affairs*. Congress No. 109, Session No. 1. April 27, 2005.

Sunstein, C.R. "Terrorism and Probability Neglect." *Journal of Risk and Uncertainty* 26(2/3) (2003): 121-136.

Swetland, Larry. *Testimony Before the New Jersey Department of Environmental Protection in the matter of Chemical Security Best Practices*. Trenton, NJ, December 1, 2005.

VROM International, Netherlands Ministry of Housing Spatial Planning and the Environment. *Safety in the Netherlands*. The Hague: Netherlands Ministry of Housing, Spatial Planning and the Environment, 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Thomas J. Mackin, Co-Advisor
   Center for Homeland Defense and Security
   Naval Postgraduate School
   Monterey, California

4. Nadav Morag, Co-Advisor
   Center for Homeland Defense and Security
   Naval Postgraduate School
   Monterey, California

5. Lisa P. Jackson, Commissioner
   New Jersey Department of Environmental Protection
   Trenton, New Jersey

6. Gary Sondermeyer, Director of Operations
   New Jersey Department of Environmental Protection
   Trenton, New Jersey

7. Nancy Wittenberg, Assistant Commissioner
   New Jersey Department of Environmental Protection
   Trenton, New Jersey

8. Jill Lipoti, Director – Division of Environmental Health and Safety
   New Jersey Department of Environmental Protection
   Trenton, New Jersey

9. Cherrie Black, Assistant Director – Infrastructure Protection
   New Jersey Office of Homeland Security and Preparedness
   Hamilton, New Jersey